Exhibit 74

atsec the information security provider

Freeman, Craft, McGregor Group

Source Code Review Report

Voting Solutions for All People (VSAP)
Version 2.0

Report Date: 2020-01-06

Version: 1.2

Status: FINAL

atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
Tel: +1 512 615 7300
Fax: +1 512 615 7301
www.atsec.com

Revision history

Version	Change date	Author(s)	Changes to previous version
1.0	2019-12-06	Ryan Hill	Initial draft
1.1	2019-12-20	Ryan Hill	Added developer response to finding #24
1.2	2020-01-06	Ryan Hill	Incorporated customer feedback

Trademarks

atsec and the atsec logo are registered trademarks of atsec information security corporation.

FCMG and the FCMG Logo are registered trademarks of the Freeman, Craft, McGregor Group.

Microsoft, Windows, .NET, and SQL Server are registered trademarks of Microsoft Corporation.

MITRE is a registered trademark of The MITRE Corporation.

Table of Contents

List of Tables

1 Executive Summary

This report was prepared by atsec information security corporation to review aspects of the security and integrity of Voting Solutions for All People (VSAP) Version 2.0. atsec is an independent, third-party company providing information-security assurance related services.

This report identifies potential security weaknesses and vulnerabilities found through static code review and searches of public vulnerability sources. The search focused particularly on those that could be exploited to alter vote recording, vote results, critical election data such as audit logs, or to conduct a denial of service attack on the voting system.

It should be noted that the public vulnerability search is most likely to identify vulnerabilities that have been reported in commonly used commercial off the shelf system components.

Reviewers performed static code analysis, including both automated scans and manual reviews of the provided source code. The code quality was found to be satisfactory, the code is well organized and generally meets the requirements of CVSS, although a few minor non-conformities were found.

Cryptographic use was also assessed. No deprecated algorithms were found to be in use. While the cryptographic code itself has been FIPS certified, it is not running on a platform that was tested for the certification. Therefore, the current use of the code does not meet the NIST standard for FIPS certification. See section 4.4, Cryptography Usage Analysis, and finding 1 in section 5.2, Static Code Analysis & Documentation Review, for details.

The code was also reviewed for the possibility of back doors. No indication of malicious code was found.

An analysis of both design and user documentation was performed. The documentation provided was found to be thorough, clear, and reasonable.

A search for public vulnerabilities was performed. Due to the high amount of third-party code, this activity returned a large number of publicly known vulnerabilities. Regardless of whether the vulnerabilities represent an actual risk to the voting system, the amount of code not controlled by the VSAP development team greatly increases the attack surface and the statistical likelihood of a problem in the future. Additions of code from external sources must always be moderated and reviewed.

After developer responses the static code analysis revealed fourteen low severity findings. For details see section 5.2, Static Code Analysis & Documentation Review.

2 Introduction

This report was prepared by atsec information security corporation to review aspects of the security and integrity of VSAP Version 2.0. It has been prepared in support of a contract awarded to Freeman, Craft, McGregor Group, Inc. This project has a goal to provide voting system test support services to assist the California Secretary of State (SOS) with the evaluation of the VSAP Version 2.0 for its suitability for use in the State of California in accordance with Elections Code sections 19001 et seq.

The source code review was performed by the following atsec information security corporation consultants.

- Ryan Hill (Project Manager/Documentation Specialist)
- King Ables (Lead Reviewer)
- Sean Lewis (Reviewer)
- Dick Sikkema (Reviewer)
- Randy Baker (Reviewer)

This document identifies the security vulnerabilities found through static code review and by searches of public vulnerability sources that could be exploited to alter vote recording, vote results, critical election data, such as audit logs, or to conduct a denial of service attack on the voting system.

2.1 Scope and Basis

VSAP Version 2.0 (hereafter referred to as the “voting system” or simply as the “system”) is a paper-based voting system made up of the following components.

- Ballot Marking Device (BMD)—The central component of the voting system and the main interface for the voter. It includes a touchscreen, an audio-tactile interface, a paper handler, a QR code scanner, a dual-switch input, and an integrated ballot box. The BMD is used by voters to generate, verify and cast paper ballots.
- BMD Manager (BMG)—Software for managing BMDs including software, ballot configurations, and post-election data.
- Enterprise Signing Authority (ESA)—A cryptographic sub-system (hardware and software) that ensures components of the VSAP conform to security standards and that the data passed to components is secure and authenticated.
- Interactive Sample Ballot (ISB)—A web application that allows prospective voters to view a digital sample ballot and mark selections with their computer or mobile device.

- Tally—Hardware and software that captures and processes ballot images ensuring that votes on paper ballots are digitally represented and counted, storing the images as Cast Vote Records (CVRs).
- VSAP Ballot Layout (VBL)—Defines ballot print formats for BMD, Vote by Mail (VBM), Remote Accessible Vote by Mail (RAVBM) and Uniformed Overseas Citizens Absentee Voting Act (UOCAVA) ballots. VBL also generates data files and packages to configure the BMD, BMG, ISB, and Tally.

atsec performed the source code review on the basis of an Agreement between Freeman, Craft, McGregor Group Inc., with the State of California, which states that the source code review includes examining the system in a manner that will provide the California Secretary of State with a basis for evaluating the extent to which the source code meets applicable standards. The threat model included in the Agreement is reproduced below and defines the threat parameters for the scope of this examination.

2.2 Inputs

The reviewers were provided with a Technical Data Package (TDP) including the source code and a set of documents that support the findings in this report. These documents were examined during the source code review to better understand the voting system and identify discrepancies between the documentation and the source code. These documents are listed in the References section.

2.3 Threat Model

This assessment is centered on the threat model given in the Request for Quotation (RFQ). The system is expected to counter the following attacks.

- Alter vote recording
- Alter vote results
- Alter critical election data, such as audit logs
- Conduct a denial of service attack on the voting system

To the extent possible, vulnerabilities found have been reported with an indication of whether the exploitation of the vulnerability would require access by any of the following.

- **Voter:** Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine(s) for less than an hour.
- **Poll worker:** Usually has low knowledge of the voting machine design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the machine(s) for up to one week, but all physical security has been put into place before the machines are received.

- **Elections official insider:** Wide range of knowledge of the voting machine design and configuration. May have unrestricted access to the machine for long periods of time. Their designated activities include:
  - Set up and pre-election procedures
  - Election operation
  - Post-election processing of results
  - Archiving and storage operations
- **Vendor insider:** Has great knowledge of the voting machine design and configuration. They have unlimited access to the machine before it is delivered to the purchaser and, thereafter, may have unrestricted access when performing warranty and maintenance service, and when providing election administration services.

The atsec team did not attempt to demonstrate exploitability of identified potential vulnerabilities. However, identified potential vulnerabilities were described along with the anticipated factors necessary to mount an attack.

2.4 Methodology

The atsec team was tasked with the source code review which included but was not limited to the following aspects.

- Evaluation of potential vulnerabilities and related issues (code quality and standards compliance), considering that an exploitable issue in a component that is not in itself security relevant could be used to subvert more critical data. This is an issue whenever the architecture of the system does not provide strong separation of the components.
- Adherence to other applicable coding format conventions and standards including best practices for the coding language used, and any IEEE, NIST, ISO or NSA standards or guidelines which the Contractor find reasonably applicable.
- Analysis of the program logic and branching structure.
- Search for exposures to commonly exploited vulnerabilities, such as buffer overflows, integer overflow, inappropriate casting or arithmetic.
- Evaluation of the use and correct implementation of cryptography and key management.
- Analysis of error and exception handling.
- Evaluation of the likelihood of security failures being detected.

  - Are audit mechanisms reliable and tamper resistant?
  - Is data that might be subject to tampering properly validated and authenticated?

- Evaluation of the risk that a user can escalate his or her capabilities beyond those authorized.

- Evaluation of whether the design and implementation follow sound, generally accepted engineering practices. Is code defensively written to protect against:

  - Bad data;
  - Errors in other modules;
  - Changes in environment;
  - User errors; and
  - Other adverse conditions.

- Evaluation of whether the system is designed in a way that allows meaningful analysis, including:

  - Is the architecture and code amenable to an external review (such as this one)?
  - Could code analysis tools be usefully applied?
  - Is the code complexity at a level that it obfuscates its logic?

- Search for embedded, exploitable code (such as “Easter eggs”) that can be triggered to affect the system.

- Search for dynamic memory access features which would permit the replacement of certificated executable code or control data or insertion of exploitable code or data.

- Search for use of runtime scripts, instructions, or other control data that can affect the operation of security relevant functions or the integrity of the data.

2.4.1 Potential vulnerabilities

The reviewers used the following public repositories to identify vulnerabilities that may affect the system.

- MITRE Common Vulnerability and Exposures (CVEs)

Although this list may not have entries for the voting system itself, constituent software and commercial off-the-shelf (COTS) components that the voting system integrates may contain vulnerabilities. The review team identified such components that the system relies upon and conducted searches for these products as well.

2.4.2 Code quality

While performing the examination of the code for other activities, the reviewers identified and recorded areas within the code base that demonstrate poor code quality. Although poor code quality does not necessarily identify vulnerabilities, it does provide an indication that vulnerabilities may exist.

The following coding standards were used during this analysis.

- California Voting System Standards, October 2014

The team also performed numerous informal static analysis activities on the source code to gather code quality data using customized command scripts.

2.4.3 Design

The source code review team used the technical data package, source code, and any material provided or otherwise publicly available to construct an understanding of the architecture and design of the voting system. This understanding included discovering the external interfaces and their security mechanisms and controls, particularly as much information as possible was gathered to support conclusions regarding the ability for a threat agent to tamper with or circumvent security controls.

Interfaces represent the primary attack surface of the voting system. Interfaces can include web-based interfaces, native graphic user interfaces, command line interfaces, or technical interfaces that are not designed for direct user interaction (e.g., database connections). Each of these interfaces was examined to identify the security controls that counter the threats.

Secure interfaces also depend on filtering out poorly structured or corrupt data. The review team specifically checked for input validation mechanisms and determined if related attacks, such as command injection are possible.

2.4.4 Cryptography

While cryptography is often the most difficult security mechanism to break directly, misuse of cryptographic primitives can render that protection weak or non-existent. The review team identified where cryptography is used throughout the source code and determined if its use is appropriate for the given purpose. For example, using a cryptographic hash function to protect passwords is appropriate while using an encryption algorithm with a hard-coded key is not.

2.4.5 Back doors

Those with access to the voting system during development and having malicious intent can place back doors into the source code so that they could gain unauthorized access to the voting system during operation. Back doors are extremely hard to find because a seasoned programmer can obfuscate code to look benign.

The review team marked areas of vulnerabilities as identified by command line searches, as described in section 4.5, for further scrutiny. For example, a particular area of code with poor code quality and access to sensitive information such as authentication credentials might be a good place to hide a back door. The reviewers gave such areas extra scrutiny by considering insider threats in addition to unintentional implementation flaws.

2.4.6 Measurement of findings

A summary of findings is listed in section 5. Each finding contains the following information.

- A description of the vulnerability or weakness
- An assessment of what threats are involved in the possible exploitation of the vulnerability or weakness
- A categorization of the findings, which can be:
  - A weakness in the source code. Weaknesses are issues identified in the source code that are not directly exploitable but may indicate the existence of exploitable vulnerabilities within the source code.
  - A non-conformity in the code quality standards. Non-conformities do not necessarily imply weaknesses, though the rationale for the requirement is often based on preventing weaknesses.
  - A potential vulnerability in the source code. The reviewers consider potential vulnerabilities to likely be exploitable.
  - A vulnerability in the source code. The reviewers have either shown or have referenced other parties who have asserted the vulnerability to be exploitable.
- A severity level of the findings, which can be either:
  - A non-finding. A non-finding indicates that investigation occurred and the results were satisfactory with no vulnerabilities detected. It may also indicate a finding which was downgraded after response or mitigation.
  - A low severity finding. Low severity implies either the impact to the product is low or already mitigated by the system, or the difficulty in exploitation would

likely require unrestricted access to the systems, expert knowledge of the system, or would require cost prohibitive resources.

- A medium severity finding. Medium severity implies either the impact of exploitation to the product would be significant, or the difficulty in exploitation would likely require extended access to the systems, informed knowledge of the system, or would require significant resources.
- A high severity finding. High severity implies either the impact of exploitation to the product would result in complete compromise of security, or the difficulty in exploitation would likely require little to no access or knowledge of the systems or little to no resources.

2.4.7 Depth of analysis

Because of the complexity and volume of the material to be reviewed, limited time available and broad scope (assessment of documents and quality of the code, along with source code review), the team concentrated on surveying a breadth of categories of vulnerabilities that they could identify, and only reviewed in depth enough samples of each of the categories to determine how that vulnerability was being handled. For all the categories, no attempt was made to enumerate how many instances existed. Other source code review projects would be likely to find more instances, but those findings should be within the listed categories.

3 Description of the VSAP Voting System

The VSAP Voting System is a suite of software, hardware, device and peripheral components for conducting and reporting elections.

3.1 Voting System Functions

The VSAP Voting System provides a number of high-level functions necessary to conduct an election. These activities include the following.

- BMD System Functions
  - Authenticate Election Worker
  - Diagnostics
  - Voting Session
  - Manage Ballots
- BMG System Functions
  - Load
  - Locate
  - Log
  - Retrieve
- ESA System Functions
  - Create Security Environment
  - Provision Certificate Authorities
  - Export Keys
- ISB System Functions
  - File Parser
  - Build Precinct to Ballot Style Map
  - Retrieve Ballot Style
  - Generate Poll Pass
  - Print UOCAVA and RAVBM Ballots
- Tally System Functions
  - Scanning
  - Recognizer
  - Load and Decrypt the BPK
  - Tabulate and Report

- VBL System Functions
    - Ballot Layout
    - Authentication Service
    - Log Viewer
    - Exporting

3.2 Physical Components

Several components are used in conducting an election with VSAP.

- **Ballot Marking Device (BMD)**—The central component of the voting system and the main interface for the voter. It includes a touchscreen, an audio-tactile interface, a paper handler, a QR code scanner, a dual-switch input, and an integrated ballot box. The BMD is used by voters to generate, verify and cast paper ballots.

- **Enterprise Signing Authority (ESA**)—A cryptographic sub-system (hardware and software) that ensures components of the VSAP conform to security standards and that the data passed to components is secure and authenticated.

- **Tally**—Hardware and software that captures and processes ballot images ensuring that votes on paper ballots are digitally represented and counted, storing the images as Cast Vote Records (CVRs).

3.3 Logical Components

- **BMD Manager (BMG)**—Software for managing BMDs including software, ballot configurations, and post-election data.

- **Interactive Sample Ballot (ISB)**—A web application that allows prospective voters to view a digital sample ballot and mark selections with their computer or mobile device.

- **VSAP Ballot Layout (VBL)**—Defines ballot print formats for BMD, Vote by Mail (VBM), Remote Accessible Vote by Mail (RAVBM) and Uniformed Overseas Citizens Absentee Voting Act (UOCAVA) ballots. VBL also generates data files and packages to configure the BMD, BMG, ISB, and Tally.

3.4 Data Interfaces

The voting system moves data between external interfaces and internal components in a variety of ways: peripheral devices, files, and databases. Table 1: Interfaces, provides detail on these interfaces.

Component	Interface	Purpose
BMD	Human interface devices	Voter selections
	USB port	Loading the OS

	Optical scanner	Authentication, ballot page metadata (BPM) and poll pass QR code input
	Ethernet interface	BMD management
	Thermal printer	marking ballots
BMG	Ethernet interface	BMD management
	USB port	Receiving security keys, election data, and ballot layout
	Human interface devices	Interacting with BMG application
	Browser-based GUI	Display and input in web browser
	Network switch	Ethernet connection to BMDs and workstations
ESA	USB port	Exporting security keys
	Human interface devices	Interacting with ESA application
ISB	Human interface devices	Interacting with ISB application
	Browser-based GUI	Display and input in web browser
	Internet interface	Online access
	Amazon Web Services	Cloud-based hosting and storage
Tally	Optical scanner	Scans and processes ballots
	Human interface devices	Interacting with Tally
	Ethernet connection to network switch	Connection to server, storage, and scanner
	Ballot feed/paper handler	Loading and processing of ballots
	USB port	Transferring security keys
VBL	Human interface devices	Interacting with VBL
	USB port	Transferring security keys, ballot files, and election data

Table 1: Interfaces

3.4.1 Network interfaces

The logical components located at the Election Central and Remote Voting sites will use ethernet for network connectivity. Election Central utilizes a closed, air-gapped network to maintain security from external attacks. Remote Voting is provided by the cloud on Amazon Web Services servers. In the Election Central environment the use of non-hardwired connectivity will not be permitted and such functionality has been disabled (e.g., wireless, Bluetooth).

The communication channels to other Election Central entities will be protected using TLS 1.2 over TCP/IP in a closed network

3.4.2 Peripheral devices

Data is moved between logical components using different media. Depending on the purpose of the data, the appropriate transport mechanism is chosen. Data will either be transported as a digital file or physically printed material. Table 1 summarizes the appropriate export media for each device or area.

Component	Export mechanism
Enterprise Signing Authority (ESA)	• Encrypted USB (Public/Private key pairs for target components)
VBL	• Encrypted USB (Voting Ballot Layouts)
Ballot Manager (BMG)	• BMG Network ◦ BMD Election Definition Upload ◦ Upload/Download of logs from BMD's ◦ Diagnostics ◦ BMD location tracking and Inventory • Encrypted USB ◦ Export BMD Security keys to Tally ◦ Import of ESA security keys ◦ Import of Trusted Build system images ◦ Import of VBL Election definitions

Ballot Marking Devices (BMD)	• Paper Ballots • Logs (Poll Close, Air-gapped Network to BMG)
Tally	• CVR's (Cast Vote Records) for tabulation from scanned Ballots • Ballot Records (Database record) • Report Data (Raw voting data)
ISB	• Poll Pass for BMD (Sample ballot marking, for quick voting at polling place) • Remote Accessible Vote by Mail Ballot (RAVBM) • Uniformed and Overseas Citizens Absentee Voting Act Ballot (UOCAVA)

Table 2: Device/Area Media

3.4.3 Files

Many file types are used by various components of the voting system and are transferred by a variety of interfaces and media. The following types of data are stored in the voting system.

- Election data and configuration files
- Media files (e.g., audio)
- Device configuration files
- Election results files
- Cast Vote Record (CVR) data files
- Audit logs
- Extensible Markup Language (XML)
- JSON files
- Database files (described below)
- Encryption and Signing Keys

3.4.4 Databases

The VSAP voting system uses SQLite 3.28, MySQL 8, and Apache Cassandra to store election data, logs, user authentication, and CVR data.

An SQLite database is only used for the BMD component, and Apache Cassandra is only used by Tally for the storage of CVR's. The following applications use MySQL databases.

- BMG
- ESA
- ISB
- VBL
- Tally

It should be noted that the different components that utilize MySQL databases for the storage of data do not share the same instance of the software. ESA, VBL, and Tally components are separately air-gapped systems, and therefore cannot share their information with other components of the voting system. ISB is hosted on Amazon Web Services servers, and therefore is unable to directly communicate with other air-gapped or secured components. Finally, BMG does not share its database information with BMD devices.

4 Static Code Analysis & Documentation Analysis

The following sections describe the assessments performed by the review team. These findings are summarized in section 5.

4.1 Design

The reviewers developed an understanding of the voting system software through the guidance and design documentation. This understanding is recorded in section 3. The reviewers used this understanding during their assessment of the source code throughout this section.

4.1.1 Components

The VSAP system is made up of the following logical and physical components.

4.1.1.1 Software

- **BMD Manager (BMG)**—Software for managing BMDs including software, ballot configurations, and post-election data.

- **Interactive Sample Ballot (ISB)**—A web application that allows prospective voters to view a digital sample ballot and mark selections with their computer or mobile device.

- **VSAP Ballot Layout (VBL)**—Defines ballot print formats for BMD, Vote by Mail (VBM), Remote Accessible Vote by Mail (RAVBM) and Uniformed Overseas Citizens Absentee Voting Act (UOCAVA) ballots. VBL also generates data files and packages to configure the BMD, BMG, ISB, and Tally.

4.1.1.2 Hardware (software also runs on these components)

- **Ballot Marking Device (BMD)**—The central component of the voting system and the main interface for the voter. It includes a touchscreen, an audio-tactile interface, a paper handler, a QR code scanner, a dual-switch input, and an integrated ballot box. The BMD is used by voters to generate, verify and cast paper ballots.

- **Enterprise Signing Authority (ESA)**—A cryptographic sub-system (hardware and software) that ensures components of the VSAP conform to security standards and that the data passed to components is secure and authenticated.

- **Tally**—Hardware and software that captures and processes ballot images ensuring that votes on paper ballots are digitally represented and counted, storing the images as Cast Vote Records (CVRs).

4.1.2 Component interfaces

The VSAP Voting System can be divided into the following three main subsystems:

- the Election Central subsystem,
- the Count subsystem, and

- the Voting subsystem.

The subsystems are not connected to each other and each implements different security related isolation measures. The Election Central subsystem only uses Ethernet for network communication (wireless capabilities are disabled). Data is transferred to and from each subsystem as either printed material (i.e., ballots) or signed, digital files on encrypted USB flash drives.

Safeguards have been put into place to mitigate and/or avoid risks during data transmission. Such examples include digitally signing files transported via encrypted USB and deploying pre-configured devices (e.g., preconfiguring BMD devices before shipment to precincts).

The interface list is small and countermeasures for potential threats are in place. This approach helps keep a reduced attack surface which is easier to manage. Chain of custody will be crucial and proper processes should be in place to ensure an audit trail for handling and transporting the USB sticks (as well as for the rest of the hardware and software).

4.1.3 Cryptographic functions

The use of cryptographic functions is of particular interest because this is the primary design feature intended to prevent unauthorized access to election data and results by poll workers and, to a lesser extent, election officials, during an election. The reviewers found problems in the design including hard-coded passwords and the use of algorithms approved by NIST, but on an Operating System not listed as an approved environment. While no single finding represents a critical vulnerability, a determined attacker might use one or more as an entry point to further incursion into the system.

4.1.4 Audit functions

All devices generate audit logs. A vulnerability for audit records is the potential for poll workers and election officials to change the system clock. This could allow for manipulation of the audit records. However, the change of time would be logged in the system log lowering the possibility of corrupting or changing the files.

4.1.5 Source code organization

Source code provided for review is predominantly Go language code with a lesser amount of JavaScript code to implement user interface components. The reviewers found the code to be generally easy to read and follow and have a logical structure. Many, though not all, source code files also include change logs at the beginning. The code was generally well commented and appropriate in most contexts.

A significant number of source code files appear to have third-party origins. Reviewers focused less attention on these, however automatic code scanning did include these files. A small number of C, C++, Python, and shell script files are also included in the source code. These were not reviewed in detail.

4.2 Published Vulnerabilities

The reviewers searched the MITRE Common Vulnerabilities and Exposures (CVE) database and the NIST NVD database for potential vulnerabilities in the system. Additionally, the reviewers searched the vendor product sites for software used within the system.

It should be noted that the public vulnerability search is most likely to identify vulnerabilities that have been reported in commonly used commercial off the shelf system components.

The following documents were used to determine the list of search terms for the public vulnerability search:

- VSAP-TDP-004 Software Design and Specification.pdf
  Version 1, Draft C – 10/14/2019
- VSAP-TDP-012_Approved_Parts_List.pdf
  Version 1, Draft B – 10/14/2019
- numerous package.json files "dependencies" list
- numerous provision.go files (rpm installs)
- rpm file names from the following sub-directories:
  - VBL_source_and_Keys/installer/rpms
  - TallySource/installer/rpms

Table 3: Component Versions and Search Terms, contains the components and versions utilized for VSAP Version 2.0 and the search terms used for the public vulnerability search.

Component	Version	Search Term
ansible	2.4.2.0-2.el7	ansible
atop	2.4.0-1.el7	atop
audit	2.8.4-4.el7	audit
audit-libs	2.8.4-4.el7	audit-libs
audit-libs-python	2.8.4-4.el7	audit-libs-python
autogen-libopts	5.18-5.el7	autogen-libopts
avahi-libs	0.6.31-19.el7	avahi-libs
Ballot Marking Device	1	Ballot Marking Device
bash	4.2.46-31.el7	bash
bind-libs	9.9.4-74.el7_6.2	bind-libs
bind-libs-lite	9.9.4-74.el7_6.2	bind-libs-lite
bind-license	9.9.4-74.el7_6.2	bind-license
bind-utils	9.9.4-74.el7_6.2	bind-utils
binutils	2.27-34.base.el7	binutils
BMG Manager	1	BMG Manager

Component	Version	Search Term
bootstrap	4.3.1	bootstrap
ca-certificates	2018.2.22-70.0.el7_5	ca-certificates
Carbon Black Linux Agent	7.4.0	Carbon Black Linux Agent
Carbon Black Server	8.1.4.98	Carbon Black Server
Carbon Black Windows Agent	8.1.5.5.70	Carbon Black Windows Agent
CentOS Linux	7.6.1810	CentOS Linux
ch.qos.logback	1.2.3	ch.qos.logback
checkpolicy	2.5-8.el7	checkpolicy
cifs-utils	6.2-10.el7	cifs-utils
cmake	2.8.12.2-2.el7	cmake
co.elastic.apm	1.9.0	co.elastic.apm
com.fasterxml.jackson.core	2.9.9	fasterxml jackson.core
com.fasterxml.jackson. dataformat	2.9.9	fasterxml jackson.dataformat
com.fasterxml.jackson. datatype	2.9.9	fasterxml jackson.datatype
com.fasterxml. jackson.module	2.9.9	fasterxml jackson.module
com.github. ulisesbocchio	2.1.1	github.ulisesbocchio
com.google.code.gson	2.8.5	google code.gson
com.google.guava	20	google guava
com.googlecode. json-simple	1.1.1	googlecode json-simple
com.itextpdf	5.5.13	itextpdf
com.melloware	1.9.4	melloware
com.zaxxer	3.2.0	zaxxer
commons-beanutils	1.9.3	commons-beanutils
commons-codec	1.11	commons-codec
commons-collections	3.2.2	commons-collections
commons-io	2.6	commons-io
commons-logging	1.2	commons-logging
conntrack-tools	1.4.4-4.el7	conntrack-tools
container-selinux	2.99-1.el7_6	container-selinux
containerd.io	1.2.5-3.1.el7	containerd.io
containerd.io	1.2.6-3.3.el7	containerd.io
coreutils	8.22-23.el7	coreutils
cri-tools	1.12.0-0	cri-tools
cronie	1.4.11-20.el7_6	cronie
cronie-anacron	1.4.11-20.el7_6	cronie-anacron

Component	Version	Search Term
cryptsetup	2.0.3-3.el7	cryptsetup
cryptsetup-libs	2.0.3-3.el7	cryptsetup-libs
cups-libs	1.6.3-35.el7	cups-libs
curl	7.29.0-51.el7_6.3	curl
dbus	1.10.24-13.el7_6	dbus
dbus-libs	1.10.24-13.el7_6	dbus-libs
de.codecentric	2.1.6	de.codecentric
device-mapper	1.02.149-10.el7_6.8	device-mapper
devtoolset-6-binutils	2.27-12.el7.1	devtoolset
devtoolset-6-gcc	6.3.1-3.1.el7	devtoolset
devtoolset-6-gcc-c++	6.3.1-3.1.el7	devtoolset
devtoolset-6-gdb	7.12.1-48.el7	devtoolset
devtoolset-6-libstdc++-devel	6.3.1-3.1.el7	devtoolset
devtoolset-6-runtime	6.1-1.el7	devtoolset
dhclient	4.2.5-68.el7.1	dhclient
dhcp-common	4.2.5-68.el7.1	dhcp-common
dhcp-libs	4.2.5-68.el7.1	dhcp-libs
dmidecode	3.1-2.el7	dmidecode
docker-ce	19.03.1-3.el7	docker-ce
docker-ce-cli	19.03.1-3.el7	docker-ce-cli
dosfstools	3.0.20-10.el7	dosfstools
dracut	033-554.el7	dracut
dracut-config-rescue	033-554.el7	dracut-config-rescue
dracut-network	033-554.el7	dracut-network
e2fsprogs	1.42.9-13.el7	e2fsprogs
e2fsprogs-libs	1.42.9-13.el7	e2fsprogs-libs
efibootmgr	17-2.el7	efibootmgr
efivar-libs	36-11.el7_6.1	efivar-libs
elfutils-default-yama-scope	0.172-2.el7	elfutils-default-yama-scope
elfutils-libelf	0.172-2.el7	elfutils-libelf
elfutils-libs	0.172-2.el7	elfutils-libs
Enterprise Signing Authority	1	Enterprise Signing Authority
ESXi	6.7	ESXi
ethtool	4.8-9.el7	ethtool
exfat-utils	1.3.0-1.el7	exfat-utils
file	5.11-35.el7	file
file-libs	5.11-35.el7	file-libs
findutils	4.5.11-6.el7	findutils

Component	Version	Search Term
firewalld	0.5.3-5.el7	firewalld
firewalld-filesystem	0.5.3-5.el7	firewalld-filesystem
freetype	2.8-12.el7_6.1	freetype
fuse-exfat	1.3.0-1.el7	fuse-exfat
fuse-libs	2.9.2-11.el7	fuse-libs
GeoIP	1.5.0-13.el7	GeoIP
git	1.8.3.1-19.el7	git
glib2	2.56.1-4.el7_6	glib2
glibc	2.17-260.el7_6.6	glibc
glibc-common	2.17-260.el7_6.6	glibc-common
gnupg2	2.0.22-5.el7_5	gnupg2
gobject-introspection	1.56.1-1.el7	gobject-introspection
gpm-libs	1.20.7-5.el7	gpm-libs
GraphicsMagick	1.3.31-2.el7	GraphicsMagick
grub2	2.02-0.76.el7.1	grub2
grub2-common	2.02-0.76.el7.1	grub2
grub2-efi-x64	2.02-0.76.el7.1	grub2
grub2-pc	2.02-0.76.el7.1	grub2
grub2-pc-modules	2.02-0.76.el7.1	grub2
grub2-tools	2.02-0.76.el7.1	grub2
grub2-tools-extra	2.02-0.76.el7.1	grub2
grub2-tools-minimal	2.02-0.76.el7.1	grub2
grubby	8.28-25.el7	grubby
gssproxy	0.7.0-21.el7	gssproxy
gtk2-devel	2.24.31-1.el7	gtk2-devel
HA-Proxy	1.5.18-8.el7	HA-Proxy
haproxy	1.5.18-8.el7	haproxy
hwdata	0.252-9.1.el7	hwdata
iftop	1.0-0.14.pre4.el7	iftop
ImageMagick	6.7.8.9-15.el7_2	ImageMagick
ImageMagick-devel	6.7.8.9-15.el7_2	ImageMagick
initscripts	9.49.46-1.el7	initscripts
Interactive Sample Ballot	1	Interactive Sample Ballot
io.micrometer	1.1.6	io.micrometer
io.netty	4.1.39.Final	io.netty
io.projectreactor	3.2.12.RELEASE	io.projectreactor
io.projectreactor.netty	0.8.11.RELEASE	io.projectreactor.netty
io.springfox	2.9.2	io.springfox

Component	Version	Search Term
io.swagger	1.5.20	io.swagger
iotop	0.6-4.el7	iotop
iproute	4.11.0-14.el7_6.2	iproute
iprutils	2.4.16.1-1.el7	iprutils
ipset	6.38-3.el7_6	ipset
ipset-libs	6.38-3.el7_6	ipset-libs
iptables	1.4.21-28.el7	iptables
ISB Client	1	ISB Client
ISB Pre-processor	1	ISB Pre-processor
java-1.8.0-openjdk	1.8.0.181-7.b13.el7	java openjdk
javax.activation	1.2.0	javax.activation
javax.annotation	1.3.2	javax.annotation
javax.persistence	2.2	javax.persistence
javax.servlet	2.4	javax.servlet
javax.transaction	1.3	javax.transaction
javax.validation	2.0.1.Final	javax.validation
javax.xml.bind	2.3.1	javax.xml.bind
jq	1.5-1.el7	jq
jsdoc	3.6.0-dev	jsdoc
json-c	0.11-4.el7_0	json-c
kbd	1.15.5-15.el7	kbd
kbd-legacy	1.15.5-15.el7	kbd
kbd-misc	1.15.5-15.el7	kbd
kernel-tools	3.10.0-957.27.2.el7	kernel-tools
kernel-tools-libs	3.10.0-957.27.2.el7	kernel-tools
kexec-tools	2.0.15-21.el7_6.4	kexec-tools
keyutils	1.5.8-3.el7	keyutils
kmod	20-23.el7	kmod
kmod-libs	20-23.el7	kmod
kpartx	0.4.9-123.el7	kpartx
krb5-libs	1.15.1-37.el7_6	krb5-libs
kubeadm	1.14.7-0	kubeadm
kubernetes-cni	0.7.5-0	kubernetes-cni
LAN Guardian Server	14.6.0.2	LAN Guardian Server
libaio	0.3.109-13.el7	libaio
libarchive	3.1.2-10.el7_2	libarchive
libbasicobjects	0.1.1-32.el7	libbasicobjects
libblkid	2.23.2-59.el7_6.1	libblkid

Component	Version	Search Term
libcgroup	0.41-20.el7	libcgroup
libcollection	0.7.0-32.el7	libcollection
libcom_err	1.42.9-13.el7	libcom_err
libcroco	0.6.12-4.el7	libcroco
libcurl	7.29.0-51.el7_6.3	libcurl
libdrm	2.4.91-3.el7	libdrm
libevent	2.0.21-4.el7	libevent
libfastjson	0.99.4-3.el7	libfastjson
libgcc	4.8.5-36.el7_6.2	libgcc
libgomp	4.8.5-36.el7_6.2	libgomp
libini_config	1.3.1-32.el7	libini_config
libldb	1.3.4-1.el7	libldb
libmount	2.23.2-59.el7_6.1	libmount
libnetfilter_cthelper	1.0.0-9.el7	libnetfilter_cthelper
libnetfilter_cttimeout	1.0.0-6.el7	libnetfilter_cttimeout
libnetfilter_queue	1.0.2-2.el7_2	libnetfilter_queue
libnfsidmap	0.25-19.el7	libnfsidmap
libpath_utils	0.2.1-32.el7	libpath_utils
libpcap	1.5.3-11.el7	libpcap
libpng	1.5.13-7.el7_2	libpng
libref_array	0.1.5-32.el7	libref_array
libreport-filesystem	2.1.11-42.el7	libreport-filesystem
libseccomp	2.3.1-3.el7	libseccomp
libselinux	2.5-14.1.el7	libselinux
libselinux-python	2.5-14.1.el7	libselinux-python
libselinux-utils	2.5-14.1.el7	libselinux-utils
libsemanage	2.5-14.el7	libsemanage
libsemanage-python	2.5-14.el7	libsemanage-python
libsepol	2.5-10.el7	libsepol
libsmartcols	2.23.2-59.el7_6.1	libsmartcols
libsmbclient	4.8.3-6.el7_6	libsmbclient
libss	1.42.9-13.el7	libss
libssh2	1.4.3-12.el7_6.3	libssh2
libstdc++	4.8.5-36.el7_6.2	libstdc++
libtalloc	2.1.13-1.el7	libtalloc
libtdb	1.3.15-1.el7	libtdb
libteam	1.27-6.el7_6.1	libteam
libtevent	0.9.36-1.el7	libtevent

Component	Version	Search Term
libtirpc	0.2.4-0.15.el7	libtirpc
libuuid	2.23.2-59.el7_6.1	libuuid
libverto-tevent	0.2.5-4.el7	libverto-tevent
libwbclient	4.8.3-6.el7_6	libwbclient
libxslt	1.1.28-5.el7	libxslt
linux-firmware	20180911-69.git85c5d90.el7	linux-firmware
lm_sensors-libs	3.4.0-6. 20160601gitf9185e5.el7	lm_sensors-libs
logrotate	3.8.6-17.el7	logrotate
lsof	4.87-6.el7	lsof
lvm2	2.02.180-10.el7_6.8	lvm2
lvm2-libs	2.02.180-10.el7_6.8	lvm2-libs
mailx	12.5-19.el7	mailx
make	3.82-23.el7	make
man-db	2.6.3-11.el7	man-db
mariadb-libs	5.5.60-1.el7_5	mariadb-libs
mdadm	4.1-rc1_2.el7	mdadm
microcode_ctl	2.1-47.5.el7_6	microcode_ctl
mokutil	15-2.el7	mokutil
MySQL	7.5.14-1.el7	MySQL cluster
nano	2.3.1-10.el7	nano
net-tools	2.0-0.24.20131004git.el7	net-tools
net.bytebuddy	1.9.16	net.bytebuddy
net.sf.supercsv	2.4.0	net.sf.supercsv
NetworkManager-libnm	1.12.0-10.el7_6	NetworkManager-libnm
nfs-utils	1.3.0-0.61.el7	nfs-utils
nginx	1.8	nginx
node-sass	4.12.0	node-sass
nodejs	8.16.0-1nodesource	nodejs
npm @babel/runtime	7.4.4	npm babel runtime
npm antlr	2.7.7	npm antlr
npm archiver	3.0.0	npm archiver
npm axios	0.19.0	npm axios
npm axios-mock-adapter	1.16.0	npm axios mock-adapter
npm babel/polyfill	7.4.4	npm babel polyfill
npm bcrypt	3.0.5	npm bcrypt
npm bindings	1.5.0	npm bindings
npm bmd-diagnostic	1.1.4	npm bmd-diagnostic

Component	Version	Search Term
npm bmd-hardware	3.0.5	npm bmd-hardware
npm bmd-sound	1.4.5	npm bmd-sound
npm bmd-tpm	1.0.8	npm bmd-tpm
npm body-parser	1.18.3	npm body-parser
npm bundle-dependencies	1.0.2	npm bundle-dependencies
npm capi	1.5.9	npm capi
npm classnames	2.2.6	npm classnames
npm colors	1.3.3	npm colors
npm compression	1.7.4	npm compression
npm core-js	2.6.5	npm core-js
npm cors	2.8.5	npm cors
npm cross-env	5.2.0	npm cross-env
npm crypto	1.0.1	npm crypto
npm date-fns	1.30.1	npm date-fns
npm diskusage	1.1.1	npm diskusage
npm dotenv	6.2.0	npm dotenv
npm electron-localshortcut	3.1.0	npm electron-localshortcut
npm electron-workers	1.10.3	npm electron-workers
npm empty-dir	1.0.0	npm empty-dir
npm enzyme	3.9.0	npm enzyme
npm enzyme-adapter-react	1.13.0	npm enzyme-adapter-react
npm eslint	5.16.0	npm eslint
npm eslint-config-airbnb	17.1.0	npm eslint-config-airbnb
npm eslint-config-prettier	6.0.0	npm eslint-config-prettier
npm eslint-plugin-prettier	3.1.0	npm eslint-plugin-prettier
npm events	3.0.0	npm events
npm express	4.16.4	npm express
npm express-logging	1.1.1	npm express-logging
npm express-zip	2.0.1	npm express-zip
npm fs-extra	7.0.1	npm fs-extra
npm getmac	1.4.6	npm getmac
npm gm	1.23.1	npm gm
npm history	4.9.0	npm history
npm html-webpack-plugin	3.2.0	npm html-webpack-plugin
npm husky	2.2.0	npm husky
npm identity-obj-proxy	3.0.0	npm identity-obj-proxy
npm jimp	0.6.4	npm jimp
npm jsdom	13.2.0	npm jsdom

Component	Version	Search Term
npm keypair	1.0.1	npm keypair
npm lint-staged	8.1.6	npm lint-staged
npm linux-os-info	2.0.0	npm linux-os-info
npm lodash	4.17.11	npm lodash
npm logops	2.1.0	npm logops
npm macaddress	0.2.9	npm macaddress
npm moment	2.24.0	npm moment
npm moment-timezone	0.5.25	npm moment-timezone
npm morgan	1.9.1	npm morgan
npm multer	1.4.1	npm multer
npm mz	2.7.0	npm mz
npm nan	2.13.2	npm nan
npm native-json	2.0.6	npm native-json
npm node-pre-gyp	0.12.0	npm node-pre-gyp
npm node-rsa	1.0.5	npm node-rsa
npm node-zbarimg	1.0.1	npm node-zbarimg
npm notosans-fontface	1.1.0	npm notosans-fontface
npm os	0.1.1	npm os
npm path	0.12.7	npm path
npm pkg	4.3.7	npm pkg
npm prettier	1.18.2	npm prettier
npm printer	0.2.2	npm printer
npm prop-types	15.7.2	npm prop-types
npm qrcode	1.3.3	npm qrcode
npm qrcode-reader	1.0.4	npm qrcode-reader
npm qrcode.react	0.9.3	npm qrcode.react
npm qs	6.7.0	npm qs
npm raw-loader	1.0.0	npm raw-loader
npm rc-input-number	4.4.2	npm rc-input-number
npm rc-tooltip	3.7.3	npm rc-tooltip
npm react	16.8.6	npm react
npm react-html-parser	2.0.2	npm react-html-parser
npm react-localization	1.0.13	npm react-localization
npm react-modal	3.8.1	npm react-modal
npm react-router	4.4.0	npm react-router
npm react-router-dom	4.4.0	npm react-router-dom
npm react-router-redux	4.0.8	npm react-router-redux
npm react-copy-to-clipboar	5.0.1	npm react-copy-to-clipboar

Component	Version	Search Term
npm react-datepicker	2.5.0	npm react-datepicker
npm react-dom	16.8.6	npm react-dom
npm react-dropzone	10.1.4	npm react-dropzone
npm react-intersection-visi	b2.1.0	npm react-intersection-visi
npm react-is	16.8.6	npm react-is
npm react-multiselect-chec	0.1.1	npm react-multiselect-chec
npm react-numeric-input	2.2.3	npm react-numeric-input
npm react-outside-click-ha	1.2.3	npm react-outside-click-ha
npm react-paginate	6.3.0	npm react-paginate
npm react-pan-and-zoom-h	2.1.2	npm react-pan-and-zoom-h
npm react-portal	4.2.0	npm react-portal
npm react-redux	7.0.3	npm react-redux
npm react-router-scroll-top	0.1.1	npm react-router-scroll-top
npm react-scripts	3.0.1	npm react-scripts
npm react-select	2.4.3	npm react-select
npm react-sortable-hoc	1.9.1	npm react-sortable-hoc
npm react-to-print	2.1.2	npm react-to-print
npm react-window	1.8.2	npm react-window
npm reactstrap	8.0.0	npm reactstrap
npm redux	4.0.1	npm redux
npm redux-devtools	3.4.1	npm redux-devtools
npm redux-thunk	2.3.0	npm redux-thunk
npm regenerator-runtime	0.13.2	npm regenerator-runtime
npm request	2.88.0	npm request
npm reselect	4.0.0	npm reselect
npm resource-router-middleware	0.6.0	npm resource-router-middleware
npm rimraf	2.6.3	npm rimraf
npm run-all	4.1.5	npm run-all
npm serialport	7.1.1	npm serialport
npm socket.io-client	2.2.0	npm socket.io-client
npm source-map-support	0.5.12	npm source-map-support
npm sox-audio	0.3.0	npm sox-audio
npm sqlite3	4.0.8	npm sqlite3
npm streaming-worker	1.0.1	npm streaming-worker
npm swagger-ui-express	3.0.10	npm swagger-ui-express
npm typeface-noto-sans	0.0.72	npm typeface-noto-sans
npm unzip	0.1.11	npm unzip

Component	Version	Search Term
npm unzip-stream	0.3.0	npm unzip-stream
npm usb	1.5.0	npm usb
npm util	0.11.1	npm util
npm vary	1.1.2	npm vary
npm winston	3.2.1	npm winston
npm winston-syslog	2.1.0	npm winston-syslog
nspr	4.19.0-1.el7_5	nspr
nss	3.36.0-7.1.el7_6	nss
nss-pem	1.0.3-5.el7_6.1	nss
nss-softokn	3.36.0-5.el7_5	nss
nss-softokn-freebl	3.36.0-5.el7_5	nss
nss-sysinit	3.36.0-7.1.el7_6	nss
nss-tools	3.36.0-7.1.el7_6	nss
nss-util	3.36.0-1.1.el7_6	nss
ntp	4.2.6p5-28.el7	ntp
ntpdate	4.2.6p5-28.el7	ntpdate
ognl	3.1.12	ognl
oniguruma	5.9.5-3.el7	oniguruma
openldap	2.4.44-21.el7_6	openldap
openscap-scanner	1.2.17-2.el7	openscap-scanner
OpenSSL	1.0.2k-16.el7	OpenSSL
org.apache.commons	3.8.1	apache.commons.lang3
org.apache. httpcomponents	4.4.12	apache. httpcomponents
org.apache.kafka	2.0.1	apache.kafka
org.apache.logging.log4j	2.11.2	apache.logging.log4j
org.apache.tomcat.embed	9.0.24	apache.tomcat.embed
org.aspectj	1.9.4	aspectj
org.atteo	1.2.2	atteo
org.attoparser	2.0.5.RELEASE	attoparser
org.codehaus.jackson	1.9.13	codehaus.jackson
org.codelibs	1.3.18.3	codelibs
org.dom4j	2.1.1	dom4j
org.glassfish	3.0.0	glassfish
org.hdrhistogram	2.1.9	hdrhistogram
org.hibernate	5.3.11.Final	hibernate
org.hibernate.common	5.0.4.Final	hibernate.common
org.hibernate.validator	6.0.17.Final	hibernate.validator

Component	Version	Search Term
org.javassist	3.20.0-GA	javassist
org.jboss	2.0.5.Final	jboss.jandex
org.jboss.logging	3.3.3.Final	jboss.logging
org.jolokia	1.6.2	jolokia
org.latencyutils	2.0.3	latencyutils
org.lz4	1.4.1	lz4
org.mapstruct	1.2.0.Final	mapstruct
org.modelmapper	2.2.0	modelmapper
org.reactivestreams	1.0.3	reactivestreams
org.slf4j	1.7.28	slf4j
org.springframework.boot	2.1.8.RELEASE	springframework.boot
org.springframework.data	2.1.10.RELEASE	springframework.data
org.springframework.hateoas	0.25.2.RELEASE	springframework.hateoas
org.springframework.integration	5.1.7.RELEASE	springframework.integration
org.springframework.kafka	2.2.8.RELEASE	springframework.kafka
org.springframework.plugin	1.2.0.RELEASE	springframework.plugin
org.springframework.retry	1.2.4.RELEASE	springframework.retry
org.springframework.security	5.1.6.RELEASE	springframework.security
org.springframework.security.oauth	2.3.6.RELEASE	springframework.seurity.oauth
org.synchronoss.cloud	1.1.3	synchronoss.cloud
org.thymeleaf	3.0.11.RELEASE	thymeleaf
org.thymeleaf.extras	3.0.4.RELEASE	thymeleaf.extras
org.unbescape	1.1.6.RELEASE	unbescape
org.xerial	3.28.0	xerial
org.xerial.snappy	1.1.7.1	xerial.snappy
org.xhtmlrenderer	9.1.18	xhtmlrenderer
Perl	5.16.3-294.el7_6	Perl
php-devel	5.4.16-46.el7	php-devel
php-pear	1.9.4-21.el7	php-pear
policycoreutils	2.5-29.el7_6.1	policycoreutils
policycoreutils-python	2.5-29.el7_6.1	policycoreutils-python
polkit	0.112-18.el7_6.1	polkit
procps-ng	3.3.10-23.el7	procps-ng

Component	Version	Search Term
psmisc	22.20-15.el7	psmisc
pytalloc	2.1.13-1.el7	pytalloc
python	2.7.5-80.el7_6	python
python2-pip	8.1.2-8.el7	python2-pip
quota	4.01-17.el7	quota
rcs	5.9.0-5.el7	rcs
rpcbind	0.2.0-47.el7	rpcbind
rpm	4.11.3-35.el7	rpm
rpm-build-libs	4.11.3-35.el7	rpm
rpm-libs	4.11.3-35.el7	rpm
rpm-python	4.11.3-35.el7	rpm-python
rsync	3.1.2-4.el7	rsync
rsyslog	8.24.0-34.el7	rsyslog
Samba	4.8.3-6.el7_6	Samba
screen	4.1.0-0.25.el7	screen
selinux-policy	3.13.1-229.el7_6.15	selinux-policy
setools-libs	3.3.8-4.el7	setools-libs
setup	2.8.71-10.el7	setup
sg3_utils	1.37-17.el7	sg3_utils
shadow-utils	4.1.5.1-25.el7_6.1	shadow-utils
shim-x64	15-2.el7	shim-x64
smartmontools	6.5-1.el7	smartmontools
Snare Central Server	7.5.0	Snare Central Server
Snare Linux Agent	5.3.1	Snare Linux Agent
Snare Windows Agent	5.3.1	Snare Windows Agent
socat	1.7.3.2-2.el7	socat
sudo	1.8.23-3.el7	sudo
sysstat	10.1.5-17.el7	sysstat
systemd	219-62.el7_6.9	systemd
systemd-libs	219-62.el7_6.9	systemd-libs
systemd-sysv	219-62.el7_6.9	systemd-sysv
Tally Digital Foundry	2	Tally Digital Foundry
tar	1.26-35.el7	tar
tcp_wrappers	7.6-77.el7	tcp_wrappers
teamd	1.27-6.el7_6.1	teamd
Terraform	1.12	Terraform
tuned	2.10.0-6.el7_6.4	tuned
tzdata	2019b-1.el7	tzdata

Component	Version	Search Term
Ubuntu Linux Server	18.04.1	Ubuntu Linux Server
util-linux	2.23.2-59.el7_6.1	util-linux
vim-common	7.4.160-5.el7	vim-common
vim-enhanced	7.4.160-5.el7	vim-enhanced
vim-filesystem	7.4.160-6.el7_6	vim-filesystem
vim-minimal	7.4.160-6.el7_6	vim-minimal
Vote Counting System	1	Vote Counting System
VSAP Ballot Layout	1	VSAP Ballot Layout
xfsprogs	4.5.0-19.el7_6	xfsprogs
xinetd	2.3.155.2	xinetd
yum	3.4.3-161.el7	yum
yum-plugin-fastestmirror	1.1.31-50.el7	yum
zbar	0.10-27.el7	zbar
zip	3.0-11.el7	zip
zlib	1.2.7-18.el7	zlib

Table 3: Component Versions and Search Terms

The results of the vulnerability search are found in section 5.1.

4.3 Code Quality

Good development practices and coding standards help make vulnerabilities easier to identify and decrease the impact of implementation flaws. The voting system claims to adhere to California Voting System Standards (CVSS). The reviewers did not explicitly validate each requirement, but performed their code review activities with these requirements in mind, and found, with a few exceptions, the code provided did consistently satisfy the requirements.

For example, CVSS section 5.1 specifies the TDP should contain software installation selections and configuration information and the reviewer found this information to have been provided. Section 7.2 requires access control be supported and lists specific requirements such as maintaining a history of passwords used, making the length of the password list configurable, and checking that the password is not set to be the same as the username. The reviewer found all these to be implemented in code. Section 7.4 requires that procedures for malware protection be documented and the reviewer found this documentation included in the TDP.

A few minor non-conformities are listed in the static code review findings in section 5.2.

In addition, code analysis tools were used to scan code for known issues. Go source code was scanned using the GoLang Lint tool found at https://github.com/golang/lint. JavaScript code was scanned using the JavaScript Lint tool found at http://javascriptlint.com. Both tools produced a number of potential issues which have been provided to the development team for their review. None are conclusive indicators of any problem and, as with most automated scan tools, review of the messages by the developer is recommended to determine if any risk exists. A summary of these results is provided in section 5.2.

VSAP leverages an unusually large number of third-party components. While good for efficient development, this does increase the risk of unforeseen flaws, side-effects, and the possibility of malicious functionality. For example, in the case of code hosted on github.com, a malicious contributor could conceivably update the code knowing it will later be imported into a version of the voting system. Care must be taken to monitor known vulnerability databases for all components not under the developer's control, either via the author's web site or a public site like https://cve.mitre.org/ and to review new code before it is imported into the VSAP development environment.

4.4 Cryptography Usage Analysis

The reviewers searched the provided documentation and source code to identify how the system implements and utilizes cryptography. During this search, the following cryptographic usage scenarios were identified.

- Storing/retrieving files
- Creating keys
- Encrypting messages/data

California Voting System Standards,7.6.1 (a), requires the use of NIST-approved algorithms and Federal Information Processing Standard (FIPS) 140-2 validated modules. The reviewers examined the source code for the cryptographic library and the choice of cryptographic primitives used within the product.

From the documentation the following certificate references for crypto libraries were found.

1747 – OpenSSL FIPS Object Module 2.0 on the following platforms:

- AcanOS 1.0 running on Feroceon 88FR131 (ARMv5) (gcc Compiler Version 4.5.3)
- AcanOS 1.0 running on Intel Core i7-3612QE (x86) with PAA (gcc Compiler Version 4.6.2)
- AcanOS 1.0 running on Intel Core i7-3612QE (x86) without PAA (gcc Compiler Version 4.6.2)
- Android 2.2 running on OMAP 3530 (ARMv7) with NEON (gcc Compiler Version 4.1.0)
- Android 2.2 running on Qualcomm QSD8250 (ARMv7) with NEON (gcc Compiler Version 4.4.0)
- Android 2.2 running on Qualcomm QSD8250 (ARMv7) without NEON (gcc Compiler Version 4.4.0)

- Android 3.0 running on NVIDIA Tegra 250 T20 (ARMv7) (gcc Compiler Version 4.4.0)
- Android 4.0 running on NVIDIA Tegra 250 T20 (ARMv7) (gcc Compiler Version 4.4.3)
- Android 4.0 running on Qualcomm Snapdragon APQ8060 (ARMv7) with NEON (gcc compiler Version 4.4.3)
- Android 4.0 running on TI OMAP 3 (ARMv7) with NEON (gcc Compiler Version 4.4.3)
- Android 4.1 running on TI DM3730 (ARMv7) with NEON (gcc Complier Version 4.6)
- Android 4.1 running on TI DM3730 (ARMv7) without NEON (gcc Compiler Version 4.6)
- Android 4.2 running on Nvidia Tegra 3 (ARMv7) with NEON (gcc Compiler Version 4.6)
- Android 4.2 running on Nvidia Tegra 3 (ARMv7) without NEON (gcc Compiler Version 4.6)
- Android 5.0 32-bit running on Qualcomm APQ8084 (ARMv7) with NEON (gcc Compiler Version 4.9)
- Android 5.0 32-bit running on Qualcomm APQ8084 (ARMv7) without NEON (gcc Compiler Version 4.9)
- Android 5.0 64-bit running on SAMSUNG Exynos7420 (ARMv8) with NEON and Crypto Extensions (gcc Compiler Version 4.9) (singleuser mode)
- Android 5.0 64-bit running on SAMSUNG Exynos7420 (ARMv8) without NEON and Crypto Extensions (gcc Compiler Version 4.9)
- Apple iOS 5.0 running on ARM Cortex A8 (ARMv7) with NEON (gcc Compiler Version 4.2.1)
- Apple iOS 5.1 running on ARMv7 (gcc Compiler Version 4.2.1)
- Apple iOS 6.1 running on Apple A6X SoC (ARMv7s) (gcc Compiler Version 4.2.1)
- Apple iOS 7.1 64- bit running on Apple A7 (ARMv8) without NEON (clang Compiler Version 5.1)
- Apple iOS 7.1 64-bit running on Apple A7 (ARMv8) with NEON (clang Compiler Version 5.1)
- Apple OS X 10.7 running on Intel Core i7-3615QM (Apple LLVM version 4.2)
- ArbOS 5.3 running on Xeon E5645 (x86) with PAA (gcc Compiler Version 4.1.2)
- ArbOS 5.3 running on Xeon E5645 (x86) without PAA (gcc Compiler Version 4.1.2)
- CascadeOS 6.1 (32 bit) running on Intel Pentium T4200 (gcc Compiler Version 4.4.5)
- CascadeOS 6.1 (64 bit) running on Intel Pentium T4200 (gcc Compiler Version 4.4.5)
- DSP Media Framework 1.4 running on TI C64x+ (TMS320C6x C/C++ Compiler v6.0.13)
- eCos 3 running on Freescale i.MX27 926ejs (ARMv5TEJ) (gcc Compiler Version 4.3.2)
- Fedora 14 running on Intel Core i5 with PAA (gcc Compiler Version 4.5.1)

- FreeBSD 10.0 running on Xeon E5- 2430L (x86) with PAA (clang Compiler Version 3.3)
- FreeBSD 10.0 running on Xeon E5-2430L (x86) without PAA (clang Compiler Version 3.3)
- FreeBSD 8.4 running on Intel Xeon E5440 (x86) 32-bit (gcc Compiler Version 4.2.1)
- FreeBSD 8.4 running on Intel Xeon E5440 (x86) without AESNI (gcc Compiler Version 4.2.1)
- FreeBSD 9.1 running on Xeon E5-2430L (x86) with PAA (gcc Compiler Version 4.2.1)
- FreeBSD 9.1 running on Xeon E5-2430L (x86) without AESNI (gcc Compiler Version 4.2.1)
- FreeBSD 9.2 running on Xeon E5-2430L (x86) with PAA (gcc Compiler Version 4.2.1)
- FreeBSD 9.2 running on Xeon E5-2430L (x86) without PAA (gcc Compiler Version 4.2.1)
- HP-UX 11i (32 bit) running on Intel Itanium 2 (HP C/aC++ B3910B)
- HP-UX 11i (64 bit) running on Intel Itanium 2 (HP C/aC++ B3910B)
- iOS 6.0 running on Apple A5 / ARM Cortex-A9 (ARMv7) with NEON (gcc Compiler Version 4.2.1)
- iOS 6.0 running on Apple A5 / ARM Cortex-A9 (ARMv7) without NEON (gcc Compiler Version 4.2.1)
- iOS 8.1 32-bit running on Apple A7 (ARMv8) with NEON (clang Compiler Version 600.0.56)
- iOS 8.1 32-bit running on Apple A7 (ARMv8) without NEON (clang Compiler Version 600.0.56)
- iOS 8.1 64-bit running on Apple A7 (ARMv8) with NEON and Crypto Extensions (clang Compiler Version 600.0.56)
- iOS 8.1 64-bit running on Apple A7 (ARMv8) without NEON and Crypto Extensions (clang Compilerv Version 600.0.56)
- Linux 2.6 running on Broadcom BCM11107 (ARMv6) (gcc Compiler Version 4.3.2)
- Linux 2.6 running on Freescale e500v2 (PPC) (gcc Compiler Version 4.4.1)
- Linux 2.6 running on Freescale PowerPCe500 (gcc Compiler Version 4.1.0)
- Linux 2.6 running on TI TMS320DM6446 (ARMv4) (gcc Compiler Version 4.3.2)
- Linux 2.6.27 running on PowerPC e300c3 (gcc Compiler Version 4.2.4)
- Linux 2.6.32 running on TI AM3703CBP (ARMv7) (gcc Compiler Version 4.3.2)
- Linux 2.6.33 running on PowerPC32 e300 (gcc Compiler Version 4.1.0)
- Linux 3.4 under Citrix XenServer 6.2 running on Intel Xeon E5-2430L with PAA (gcc Compiler Version 4.8.0)
- Linux 3.4 under Citrix XenServer 6.2 running on Intel Xeon E5-2430L without PAA (gcc Compiler Version 4.8.0)
- Linux 3.4 under Microsoft Windows 2012 Hyper-V running on Intel Xeon E5-2430L with PAA (gcc Compiler Version 4.8.0)2
- Linux 3.4 under Microsoft Windows 2012 Hyper-V running on Intel Xeon E5-2430L without PAA (gcc Compiler Version 4.8.0)

- Linux 3.4 under Vmware ESXi 5.1 running on Intel Xeon E5-2430L with PAA (gcc Compiler Version 4.8.0)
- Linux 3.4 under Vmware ESXi 5.1 running on Intel Xeon E5-2430L without PAA (gcc Compiler Version 4.8.0)
- Linux 3.8 running on ARM926 (ARMv5TEJ) (gcc Compiler Version 4.7.3)
- Linux ORACLESP 2.6 running on ASPEED AST-Series (ARMv5) (gcc Compiler Version 4.4.5)
- Linux ORACLESP 2.6 running on Emulex PILOT3 (ARMv5) (gcc Compiler Version 4.4.5)
- Microsoft Windows 7 (32 bit) running on Intel Celeron (Microsoft 32 bit C/C++ Optimizing Compiler Version 16.00)
- Microsoft Windows 7 (64 bit) running on Intel Pentium 4 (Microsoft C/C++ Optimizing Compiler Version 16.00)
- Microsoft Windows 7 running on Intel Core i5- 2430M (64-bit) with PAA (Microsoft ® C/C++ Optimizing Compiler Version 16.00 for x64)
- Microsoft Windows CE 5.0 running on ARMv7 (Microsoft C/C++ Optimizing Compiler Version 13.10 for ARM)
- Microsoft Windows CE 6.0 running on ARMv5TEJ (Microsoft C/C++ Optimizing Compiler Version 15.00 for ARM)
- NetBSD 5.1 running on Intel Xeon 5500 (gcc Compiler Version 4.1.3)
- NetBSD 5.1 running on PowerPCe500 (gcc Compiler Version 4.1.3)
- OpenWRT 2.6 running on MIPS 24Kc (gcc Compiler Version 4.6.3)
- Oracle Linux 5 (64 bit) running on Intel Xeon 5675 (gcc Compiler Version 4.1.2)
- Oracle Linux 5 running on Intel Xeon 5675 with PAA (gcc Compiler Version 4.1.2)
- Oracle Linux 6 running on Intel Xeon 5675 with PAA (gcc Compiler Version 4.4.6)
- Oracle Linux 6 running on Intel Xeon 5675 without PAA (gcc Compiler Version 4.4.6)
- Oracle Solaris 10 (32 bit) running on SPARC-T3 (SPARCv9) (gcc Compiler Version3.4.3)
- Oracle Solaris 10 (64 bit) running on SPARC-T3 (SPARCv9) (gcc Compiler Version 3.4.3)
- Oracle Solaris 11 (32 bit) running on Intel Xeon 5675 (gcc Compiler Version 4.5.2)
- Oracle Solaris 11 (32 bit) running on SPARC-T3 (SPARCv9) (Sun C Version 5.12)
- Oracle Solaris 11 (64 bit) running on Intel Xeon 5675 (gcc Compiler Version 4.5.2)
- Oracle Solaris 11 (64 bit) running on SPARC-T3 (SPARCv9) (Sun C Version 5.12)
- Oracle Solaris 11 running on Intel Xeon 5675 with AESNI (32 bit) (gcc Compiler Version 4.5.2)
- Oracle Solaris 11 running on Intel Xeon 5675 with AESNI (64 bit) (gcc Compiler Version 4.5.2)
- PexOS 1.0 under vSphere ESXi 5.1 running on Intel Xeon E52430L with PAA (gcc Compiler Version 4.6.3)3
- PexOS 1.0 under vSphere ESXi 5.1 running on Intel Xeon E52430L without PAA (gcc Compiler Version 4.6.3)
- QNX 6.4 running on Freescale i.MX25 (ARMv4) (gcc Compiler Version 4.3.3)
- QNX 6.5 running on Freescale i.MX25 (ARMv4) (gcc Compiler Version 4.3.3)

- TS-Linux 2.4 running on Arm920Tid (ARMv4) (gcc Compiler Version 4.3.2)4
- Ubuntu 10.04 (32 bit) running on Intel Pentium T4200 (gcc Compiler Version 4.1.3)
- Ubuntu 10.04 (64 bit) running on Intel Pentium T4200 (gcc Compiler Version 4.1.3)
- Ubuntu 10.04 running on Intel Core i5 with PAA (32 bit) (gcc Compiler Version 4.1.3)
- Ubuntu 10.04 running on Intel Pentium T4200 (gcc Compiler Version 4.1.3)
- Ubuntu 13.04 running on AM335x Cortex-A8 (ARMv7) with NEON (gcc Compiler Version 4.7.3)
- Ubuntu 13.04 running on AM335x Cortex-A8 (ARMv7) without NEON (gcc Compiler Version 4.7.3)
- uCLinux 0.9.29 running on ARM 922T (ARMv4) (gcc Compiler Version 4.2.1)
- Vmware Horizon Workspace 1.5 under Vmware ESXi 5.0 running on Intel Xeon E3-1220 (x86) with PAA (gcc Compiler Version 4.5.1)1
- Vmware Horizon Workspace 1.5 under Vmware ESXi 5.0 running on Intel Xeon E3-1220 (x86) without PAA (gcc Compiler Version 4.5.1)
- Vmware Horizon Workspace 2.1 under vSphere ESXi 5.5 running on Intel Xeon E3-1220 (x86) with PAA (gcc Compiler Version 4.5.1)
- Vmware Horizon Workspace 2.1 under vSphere ESXi 5.5 running on Intel Xeon E3-1220 (x86) without PAA (gcc Compiler Version 4.5.1)
- VxWorks 6.8 running on TI TNETV1050 (MIPS) (gcc Compiler Version 4.1.2)
- VxWorks 6.9 running on Freescale P2020 (PPC) (gcc Compiler Version 4.3.3)
- Windows Embedded Compact 7 running on Freescale i.MX53xA (ARMv7) with NEON (Microsoft C/C++ Optimizing Compiler Version 15.00.20720)
- Windows Embedded Compact 7 running on Freescale i.MX53xD (ARMv7) with NEON (Microsoft C/C++ Optimizing Compiler Version 15.00.20720)

The tested configuration stated for this evaluation was CentOS 7.6.1810. It is a requirement for FIPS validation to only use modules which are used on one of the tested configurations listed on the certificate.

The CMVP Validation list is found at: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/1747.

4.4.1 Algorithms

Table 4: VSAP Algorithms, details the algorithms found in the source code.

Algorithm	Usage	Assessment
RSA Signature Generation/ Verification	**Implementation: key.go** **Usage example:** _key.SignPKCS1v15(hashType, data) key.VerifyPKCS1v15(hashType, data,	Use of a 2048-bit key and SHA-256

Algorithm	Usage	Assessment
	sig)	
SHA-256	**Implementation: proxy.go** **Usage example:** openssl.NewSHA256Hash()	For FIPS 140-2, Secure Hash Algorithm (SHA)-256 is an approved algorithm for hashing.

Table 4: VSAP Algorithms

4.5 Back Doors

A "back door" is functionality either accidentally or intentionally added to source code allowing undocumented access to, or bypassing of, established security mechanisms of running software. A competent developer may be able to obfuscate their modifications so that they are not noticeable in casual observation.

While most findings in this report are assumed to be mistakes or oversights, it is possible one or more could have been added intentionally. For example, a weak or broken cryptographic algorithm could have been deliberately added to the source base by a developer to facilitate a specific attack. Is the use of SHA-1 a back door or merely a failure to stay current with approved algorithms? It is not possible to measure the motivations of the developer from the source code. Without some clear indicator, no particular finding can be assumed to be a back door.

A back door also need not be deliberately added to the source code in order for it to exist. Simply having knowledge of unfixed bugs identified in the source code could be enough to violate the security properties of the system.

The VSAP voting system is implemented in multiple languages and many thousands of lines of code. In any system this complex, a thorough examination for back doors is not possible. However, it is reasonable to look for some classic indicators of odd behavior or obfuscation, such as the following.

- Complex constant definitions
- Use of apparently inappropriate constant values
- Strange formatting of code around control structures, loops, or branches
- Use of remote execution calls
- Use of calls to grant permission jump or passthrough

The reviewer also examined areas of code implementing data transfers over the interfaces previously described. After becoming familiar with the source code, the reviewers assessed the possibility of a back door. While it is extremely difficult to prove a negative, that no back doors exist in a system, no indications of back doors based on the above criteria were found. The reviewers examined the general look and format of the source code and found nothing considered to be out of the ordinary.

This assessment only applies to the source code included for review. It is possible the tools and systems used to build the voting system software could themselves have been attacked and made to introduce aberrant behavior into the system, independent of the source code reviewed.

4.6 Documentation Analysis

4.6.1 Technical Specifications

The technical specifications for the system was analyzed in the course of performing the source code analysis activities.

Table 5: Summary of Technical Specifications, details the technical specifications present in the TDP.

Title	Revision	Filename
Configuration Management Plan	Version 1, Draft B (07/15/2019)	VSAP-CMP-001_Configuration_ Management_Plan.pdf
Configuration Management Plan Conformity Matrix TDP	Version B, Draft B (07/15/2019)	VSAP-CMP-001-C_Configuration_ Management_Plan_Conformity_ Matrix.pdf
System Overview TDP	Version 1, Draft C 10/14/2019	VSAP-TDP-001_System_Overview.pdf
System Overview Conformity Matrix TDP	Version 1, Draft B (07/15/2019)	VSAP-TDP-001-C_System_Overview_ Conformity_Matrix.pdf
System Functionality Description TDP	Version 1, Draft B (07/15/2019)	VSAP-TDP-002_System_ Functionality_Description.pdf
System Functionality Description Conformity Matrix TDP	Version 1, Draft B (07/15/2019)	VSAP-TDP-002-C_System_ Functionality_Conformity_Matrix.pdf
System Hardware Specification TDP	Version 1, Draft E (09/12/2019)	VSAP-TDP-003 System Hardware Specification.pdf
System Hardware Specification Conformity Matrix TDP	Version 1, Draft B (07/15/2019)	VSAP-TDP-003-C System Hardware Conformity Matrix.pdf
Software Design and Specification TDP	Version 1, Draft C (10/14/2019)	VSAP-TDP-004 Software Design and Specification.pdf
Software Design and Specification – Interface Description TDP	Version 1, Draft C (09/25/2019)	VSAP-TDP-004-01_Interface_Description.pdf

Title	Revision	Filename
Software Design and Specification Conformity TDP	Version 1, Draft B (07/15/2019)	VSAP-TDP-004-C_Software_Design_and_Specification_Conformity_Matrix.pdf
System Security Specification TDP	Version 1, Draft C (09/25/2019)	VSAP-TDP-005 System_Security_Specification.pdf
System Security Specification Conformity Matrix TDP	Version 1, Draft C (09/25/2019)	VSAP-TDP-005-C_System_Security_Conformity_Matrix.pdf
System Test and Verification Specification TDP	Version 1, Draft C (10/14/2019)	VSAP-TDP-006_System_Test_and_Verification_Specification.pdf
System Operations Procedures TDP	Version 1, Draft B (07/15/2019)	VSAP-TDP-007_System_Operations_Procedures.pdf
System Operations Procedures Conformity Matrix TDP	Version, Draft B (07/15/2019)	VSAP-TDP-007-C_System_Operations_Procedures_Conformity_Matrix.pdf
System Maintenance TDP	Version 1, Draft B (07/15/2019)	VSAP-TDP-008_System_Maintenance_Manual.pdf
System Maintenance Conformity Matrix TDP	Version 1, Draft B (07/15/2019)	VSAP-TDP-008-C_System_Maintenance_Manual_Conformity_Matrix.pdf
System Maintenance TDP	Version 1, Draft B (07/15/2019)	VSAP-TDP-008_System_Maintenance_Manual.pdf
Personnel Deployment and Training Requirements Conformity Matrix TDP	Version 1, Draft B (07/15/2019)	VSAP-TDP-009-C_Personnel_Deployment_Training_Conformity_Matrix.pdf
Personnel Deployment and Training Requirements TDP	Version 1, Draft B (07/15/2019)	VSAP-TDP-009-C_Personnel_Deployment_Training_Requirements.pdf
Configuration Audits Conformity Matrix TDP	Version 1, Draft A (07/15/2019)	VSAP-TDP-010-C_Configuration_Audits_Conformity_Matrix.pdf
Configuration Audits TDP	Version 1, Draft A (07/15/2019)	VSAP-TDP-010- Configuration_Audits.pdf
Acronyms and Definitions TDP	Version 1, Draft B (07/15/2019)	VSAP-TDP-011_Acronyms_and_Definitions.pdf

Title	Revision	Filename
Approved Parts List TDP	Version 1, Draft C (11/18/2019)	VSAP-TDP-012_Approved_Parts_List.pdf

Table 5: Summary of Technical Specifications

The analysis found that the design documentation is thorough, clear, reasonable, and describes the system as it exists in the source code.

4.6.2 User Guides

The user guides for the system were analyzed in the course of performing the source code analysis activities. Table 6: Summary of User Guides, details the user guides present in the TDP.

Title	Revision	Filename
Use Procedures	Version 4 (11/2/2019)	VSAP_UPM_001_Ver4.pdf
Ballot Marking Device (BMD) User Guide	Version 4	BMD_USG_002_Rev4.pdf
Ballot Marking Device Manager (BMG) Installation Guide	Version 2	BMG Installation Procedures-v2-20190715_215423.pdf
BMD Manager User Guide	Version 4 (10/23/2019)	VSAP-USG-003 BMG User Guide.pdf
BMD Solution Applications Build Procedures	Version 0.2 (10/14/2019)	VSAP-USG-014 BMD Solution Applications Build Procedures.pdf
BMD Solution OS Build Procedures	Version 0.4 (12/10/2019)	VSAP-USG-015 BMD Solution OS Build Procedures.pdf
Carbon Black Agent Deployment for Windows – BMG	Version 0.2 (11/1/2019)	VSAP-USG-028 Carbon black Agent Deployment for Windows-BMG.pdf
Carbon Black Enabling Protection – BMG	Version 0.2 (11/1/2019)	VSAP-USG-031 Carbon Black Enabling Protection-BMG.pdf
Carbon Black Uninstall Guide	Version 0.1 (11/4/2019)	VSAP-USG-048 Carbon Black Uninstall Guide.pdf
Deployment Laptop Build Procedures	Version 0.1 (10/14/2019)	VSAP-USG-020 Deployment Laptop Build Procedures.pdf
Digital Signing Authority (DSA) Server Build/Installation	Version 2	DSA_BuildInstall_USG_012_Vers2.pdf
Digital Signing Authority (DSA) User Guide	Version 2	DSA_USG_007_Rev2.pdf
FormatOS Deployment Guide	Version 0.4 (11/1/2019)	VSAP-USG-016 FormatOS Deployment Guide.pdf

Title	Revision	Filename
Interactive Sample Ballot Pre-Processor User Guide	Version 4	VSAP_USG_001_Rev4.pdf
Interactive Sample Ballot User Guide	Version 4	VSAP_USG_004_Rev4.pdf
ISB Installation Guide	Version 0.1 (09/05/2019)	VSAP-USG-006 ISB Installation Guide.pdf
Secure Boot Tools Build Procedures	Version 0.3 (12/10/2019)	VSAP-USG-013 Secure Boot Tools Build Procedures.pdf
BMG Deployment Guide	Version 0.1 (07/16/2019)	VSAP-USG-017 BMG Deployment Guide
Snare Server Installation Guide – BMG and Tally	Version 0.2 (11/1/2019)	VSAP-USG-022 Snare Server Installation Guide – BMG and Tally.pdf
Tally Build / Installation User Guide	Version 2	Tally_Build_Install_USG_008_Rev2.pdf
Tally User Guide	Version 2	Tally_USG_009_Rev2.pdf
Ubuntu Server Installation Guide	Version 0.1 (10/14/2019)	VSAP-USG-019 Ubuntu Server Installation Guide.pdf
Ballot Layout Build / Installation User Guide	Version 2	VBL_BuildInstall_USG_011_Rev2.pdf
Ballot Layout User Guide	Version 2	VBL_USG_010_Rev2.pdf
Carbon Black Server Installation Guide - BMG	Version 2.0 (11/1/2019)	VSAP-USG-021 BMG Carbon Black Server Installation Guide.pdf

Table 6: Summary of User Guides

The analysis found that the user guidance is clear and reasonable and describes the functions of the system, the interfaces, and how to configure the system securely.

5 Findings

5.1 Public Vulnerability Search

Table 7: Potential Vulnerabilities Identified lists the publicly known vulnerabilities identified that could potentially impact the voting system. Only CVEs applicable to software versions used by the voting system are included in the results. It is recommended that the developers review each CVE and evaluate the threat each one represents.

Vulnerability	Description
ansible 2.4.2.0-2.el7	
CVE-2018-10855	Ansible 2.5 prior to 2.5.5, and 2.4 prior to 2.4.5, do not honor the no_log task flag for failed tasks. When the no_log flag has been used to protect sensitive data passed to a task from being logged, and that task does not run successfully, Ansible will expose sensitive data in log files and on the terminal of the user running Ansible.
CVE-2019-10156	A flaw was discovered in the way Ansible templating was implemented in versions before 2.6.18, 2.7.12 and 2.8.2, causing the possibility of information disclosure through unexpected variable substitution. By taking advantage of unintended variable substitution the content of any variable may be disclosed.
google guava 20	
CVE-2018-10237	Unbounded memory allocation in Google Guava 11.0 through 24.x before 24.1.1 allows remote attackers to conduct denial of service attacks against servers that depend on this library and deserialize attacker-provided data, because the AtomicDoubleArray class (when serialized with Java serialization) and the CompoundOrdering class (when serialized with GWT serialization) perform eager allocation without appropriate checks on what a client has sent and whether the data size is reasonable.
hibernate 5.3.11.Final	
CVE-2017-7536	In Hibernate Validator 5.2.x before 5.2.5 final, 5.3.x, and 5.4.x, it was found that when the security manager's reflective permissions, which allows it to access the private members of the class, are granted to Hibernate Validator, a potential privilege escalation can occur. By allowing the calling code to access those private members without the permission an attacker may be able to validate an invalid instance and access the private member value via ConstraintViolation#getInvalidValue().
npm lodash 4.17.11	
CVE-2019-10744	Versions of lodash lower than 4.17.12 are vulnerable to Prototype Pollution. The function defaultsDeep could be tricked into adding or modifying properties of Object.prototype using a constructor payload.
lz4 1.4.1	
CVE-2019-17543	LZ4 before 1.9.2 has a heap-based buffer overflow in LZ4_write32 (related to LZ4_compress_destSize), affecting applications that call LZ4_compress_fast with a large input. (This issue can also lead to data corruption.) NOTE: the vendor states "only a few specific / uncommon usages of the API are at risk."
npm moment 2.24.0	
CVE-2016-4055	The duration function in the moment package before 2.11.2 for Node.js allows remote attackers to cause a denial of service (CPU consumption) via a long string, aka a "regular expression Denial of Service (ReDoS)."
CVE-2017-18214	The moment module before 2.19.3 for Node.js is prone to a regular expression denial of service via a crafted date string, a different vulnerability than CVE-2016-4055.

nginx 1.8	
CVE-2016-0742	The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (invalid pointer dereference and worker process crash) via a crafted UDP DNS response.
CVE-2016-0746	Use-after-free vulnerability in the resolver in nginx 0.6.18 through 1.8.0 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (worker process crash) or possibly have unspecified other impact via a crafted DNS response related to CNAME response processing.
CVE-2016-0747	The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 does not properly limit CNAME resolution, which allows remote attackers to cause a denial of service (worker process resource consumption) via vectors related to arbitrary name resolution.
CVE-2018-16845	nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.
slf4j 1.7.28	
CVE-2018-8088	org.slf4j.ext.EventData in the slf4j-ext module in QOS.CH SLF4J before 1.8.0-beta2 allows remote attackers to bypass intended access restrictions via crafted data.
ESXi 6.7	
CVE-2018-6965	VMware ESXi (6.7 before ESXi670-201806401-BG), Workstation (14.x before 14.1.2), and Fusion (10.x before 10.1.2) contain an out-of-bounds read vulnerability in the shader translator. Successful exploitation of this issue may lead to information disclosure or may allow attackers with normal user privileges to crash their VMs, a different vulnerability than CVE-2018-6966 and CVE-2018-6967.
CVE-2018-6966	VMware ESXi (6.7 before ESXi670-201806401-BG), Workstation (14.x before 14.1.2), and Fusion (10.x before 10.1.2) contain an out-of-bounds read vulnerability in the shader translator. Successful exploitation of this issue may lead to information disclosure or may allow attackers with normal user privileges to crash their VMs, a different vulnerability than CVE-2018-6965 and CVE-2018-6967.
CVE-2018-6967	VMware ESXi (6.7 before ESXi670-201806401-BG), Workstation (14.x before 14.1.2), and Fusion (10.x before 10.1.2) contain an out-of-bounds read vulnerability in the shader translator. Successful exploitation of this issue may lead to information disclosure or may allow attackers with normal user privileges to crash their VMs, a different vulnerability than CVE-2018-6965 and CVE-2018-6966.
CVE-2018-6972	VMware ESXi (6.7 before ESXi670-201806401-BG, 6.5 before ESXi650-201806401-BG, 6.0 before ESXi600-201806401-BG and 5.5 before ESXi550-201806401-BG), Workstation (14.x before 14.1.2), and Fusion (10.x before 10.1.2) contain a denial-of-service vulnerability due to NULL pointer dereference issue in RPC handler. Successful exploitation of this issue may allow attackers with normal user privileges to crash their VMs.
CVE-2018-6974	VMware ESXi (6.7 before ESXi670-201810101-SG, 6.5 before ESXi650-201808401-BG, and 6.0 before ESXi600-201808401-BG), Workstation (14.x before 14.1.3) and Fusion (10.x before 10.1.3) contain an out-of-bounds read vulnerability in SVGA device. This issue may allow a guest to execute code on the host.
CVE-2018-6977	VMware ESXi (6.7, 6.5, 6.0), Workstation (15.x and 14.x) and Fusion (11.x and

	10.x) contain a denial-of-service vulnerability due to an infinite loop in a 3D-rendering shader. Successfully exploiting this issue may allow an attacker with normal user privileges in the guest to make the VM unresponsive, and in some cases, possibly result other VMs on the host or the host itself becoming unresponsive.
CVE-2018-6981	VMware ESXi 6.7 without ESXi670-201811401-BG and VMware ESXi 6.5 without ESXi650-201811301-BG, VMware ESXi 6.0 without ESXi600-201811401-BG, VMware Workstation 15, VMware Workstation 14.1.3 or below, VMware Fusion 11, VMware Fusion 10.1.3 or below contain uninitialized stack memory usage in the vmxnet3 virtual network adapter which may allow a guest to execute code on the host.
CVE-2018-6982	VMware ESXi 6.7 without ESXi670-201811401-BG and VMware ESXi 6.5 without ESXi650-201811301-BG contain uninitialized stack memory usage in the vmxnet3 virtual network adapter which may lead to an information leak from host to guest.
CVE-2019-5516	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6), Fusion (11.x before 11.0.3 and 10.x before 10.1.6) updates address an out-of-bounds vulnerability with the vertex shader functionality. Exploitation of this issue requires an attacker to have access to a virtual machine with 3D graphics enabled. Successful exploitation of this issue may lead to information disclosure or may allow attackers with normal user privileges to create a denial-of-service condition on their own VM. The workaround for this issue involves disabling the 3D-acceleration feature. This feature is not enabled by default on ESXi and is enabled by default on Workstation and Fusion.
CVE-2019-5517	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6), Fusion (11.x before 11.0.3 and 10.x before 10.1.6) contain multiple out-of-bounds read vulnerabilities in the shader translator. Exploitation of these issues requires an attacker to have access to a virtual machine with 3D graphics enabled. Successful exploitation of these issues may lead to information disclosure or may allow attackers with normal user privileges to create a denial-of-service condition on their own VM. The workaround for these issues involves disabling the 3D-acceleration feature. This feature is not enabled by default on ESXi and is enabled by default on Workstation and Fusion.
CVE-2019-5518	VMware ESXi (6.7 before ESXi670-201903001, 6.5 before ESXi650-201903001, 6.0 before ESXi600-201903001), Workstation (15.x before 15.0.4, 14.x before 14.1.7), Fusion (11.x before 11.0.3, 10.x before 10.1.6) contain an out-of-bounds read/write vulnerability in the virtual USB 1.1 UHCI (Universal Host Controller Interface). Exploitation of this issue requires an attacker to have access to a virtual machine with a virtual USB controller present. This issue may allow a guest to execute code on the host.
CVE-2019-5519	VMware ESXi (6.7 before ESXi670-201903001, 6.5 before ESXi650-201903001, 6.0 before ESXi600-201903001), Workstation (15.x before 15.0.4, 14.x before 14.1.7), Fusion (11.x before 11.0.3, 10.x before 10.1.6) contain a Time-of-check Time-of-use (TOCTOU) vulnerability in the virtual USB 1.1 UHCI (Universal Host Controller Interface). Exploitation of this issue requires an attacker to have access to a virtual machine with a virtual USB controller present. This issue may allow a guest to execute code on the host.
CVE-2019-5520	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6), Fusion (11.x before 11.0.3 and 10.x before 10.1.6) updates address an out-of-bounds read vulnerability. Exploitation of this issue requires an attacker to have access to a virtual machine with 3D graphics enabled. Successful exploitation of this issue may lead to information disclosure.The workaround for this issue

	involves disabling the 3D-acceleration feature. This feature is not enabled by default on ESXi and is enabled by default on Workstation and Fusion.
CVE-2019-5521	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6) and Fusion (11.x before 11.0.3 and 10.x before 10.1.6) contain an out-of-bounds read vulnerability in the pixel shader functionality. Successful exploitation of this issue may lead to information disclosure or may allow attackers with normal user privileges to create a denial-of-service condition on the host. Exploitation of this issue require an attacker to have access to a virtual machine with 3D graphics enabled. It is not enabled by default on ESXi and is enabled by default on Workstation and Fusion.
CVE-2019-5531	VMware vSphere ESXi (6.7 prior to ESXi670-201810101-SG, 6.5 prior to ESXi650-201811102-SG, and 6.0 prior to ESXi600-201807103-SG) and VMware vCenter Server (6.7 prior to 6.7 U1b, 6.5 prior to 6.5 U2b, and 6.0 prior to 6.0 U3j) contain an information disclosure vulnerability in clients arising from insufficient session expiration. An attacker with physical access or an ability to mimic a websocket connection to a user&#8217
CVE-2019-5536	VMware ESXi (6.7 before ESXi670-201908101-SG and 6.5 before ESXi650-201910401-SG), Workstation (15.x before 15.5.0) and Fusion (11.x before 11.5.0) contain a denial-of-service vulnerability in the shader functionality. Successful exploitation of this issue may allow attackers with normal user privileges to create a denial-of-service condition on their own VM. Exploitation of this issue require an attacker to have access to a virtual machine with 3D graphics enabled. It is not enabled by default on ESXi and is enabled by default on Workstation and Fusion.
MySQL cluster 7.5.14-1.el7	
CVE-2017-3304	Vulnerability in the MySQL Cluster component of Oracle MySQL (subcomponent: Cluster: DD). Supported versions that are affected are 7.2.27 and earlier, 7.3.16 and earlier, 7.4.14 and earlier and 7.5.5 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L).
CVE-2017-3321	Vulnerability in the MySQL Cluster component of Oracle MySQL (subcomponent: Cluster: General). Supported versions that are affected are 7.2.19 and earlier, 7.3.8 and earlier and 7.4.5 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS v3.0 Base Score 3.7 (Availability impacts).
OpenSSL 1.0.2k-16.el7	
CVE-2017-3735	While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.
CVE-2017-3736	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key

	may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.
CVE-2017-3737	OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.
CVE-2017-3738	There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.
CVE-2018-0732	During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).
CVE-2018-0734	The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).
CVE-2018-0737	The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).
CVE-2018-0739	Constructed ASN.1 types with a recursive definition (such as can be found in

	PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).
CVE-2019-1547	Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).
CVE-2019-1552	OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).
CVE-2019-1559	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q).
CVE-2019-1563	In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack.

	Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).
Perl 5.16	
CVE-2012-6329	The _compile function in Maketext.pm in the Locale::Maketext implementation in Perl before 5.17.7 does not properly handle backslashes and fully qualified method names during compilation of bracket notation, which allows context-dependent attackers to execute arbitrary commands via crafted input to an application that accepts translation strings from users.
CVE-2013-1667	The rehash mechanism in Perl 5.8.2 through 5.16.x allows context-dependent attackers to cause a denial of service (memory consumption and crash) via a crafted hash key.
CVE-2016-1238	(1) cpan/Archive-Tar/bin/ptar, (2) cpan/Archive-Tar/bin/ptardiff, (3) cpan/Archive-Tar/bin/ptargrep, (4) cpan/CPAN/scripts/cpan, (5) cpan/Digest-SHA/shasum, (6) cpan/Encode/bin/enc2xs, (7) cpan/Encode/bin/encguess, (8) cpan/Encode/bin/piconv, (9) cpan/Encode/bin/ucmlint, (10) cpan/Encode/bin/unidump, (11) cpan/ExtUtils-MakeMaker/bin/instmodsh, (12) cpan/IO-Compress/bin/zipdetails, (13) cpan/JSON-PP/bin/json_pp, (14) cpan/Test-Harness/bin/prove, (15) dist/ExtUtils-ParseXS/lib/ExtUtils/xsubpp, (16) dist/Module-CoreList/corelist, (17) ext/Pod-Html/bin/pod2html, (18) utils/c2ph.PL, (19) utils/h2ph.PL, (20) utils/h2xs.PL, (21) utils/libnetcfg.PL, (22) utils/perlbug.PL, (23) utils/perldoc.PL, (24) utils/perlivp.PL, and (25) utils/splain.PL in Perl 5.x before 5.22.3-RC2 and 5.24 before 5.24.1-RC2 do not properly remove . (period) characters from the end of the includes directory array, which might allow local users to gain privileges via a Trojan horse module under the current working directory. CVE-2016-1283
CVE-2017-12814	Stack-based buffer overflow in the CPerlHost::Add method in win32/perlhost.h in Perl before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 on Windows allows attackers to execute arbitrary code via a long environment variable.
CVE-2017-12837	Heap-based buffer overflow in the S_regatom function in regcomp.c in Perl 5 before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to cause a denial of service (out-of-bounds write) via a regular expression with a '\N{}' escape and the case-insensitive modifier.
CVE-2017-12883	Buffer overflow in the S_grok_bslash_N function in regcomp.c in Perl 5 before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to disclose sensitive information or cause a denial of service (application crash) via a crafted regular expression with an invalid '\N{U+...}' escape.
CVE-2018-18311	Perl before 5.26.3 and 5.28.x before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.
CVE-2018-18312	Perl before 5.26.3 and 5.28.0 before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.
CVE-2018-18313	Perl before 5.26.3 has a buffer over-read via a crafted regular expression that triggers disclosure of sensitive information from process memory.
CVE-2018-18314	Perl before 5.26.3 has a buffer overflow via a crafted regular expression that triggers invalid write operations.
Python 2.7.5-80.el7_6	
CVE-2018-14647	Python's elementtree C accelerator failed to initialise Expat's hash salt during initialization. This could make it easy to conduct denial of service attacks against Expat by constructing an XML document that would cause pathological hash collisions in Expat's internal data structures, consuming large amounts CPU and RAM. Python 3.8, 3.7, 3.6, 3.5, 3.4, 2.7 are believed to be vulnerable.
CVE-2018-20852	http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py in

	Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., pythonicexample.com to steal cookies for example.com). When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.
CVE-2019-10160	A security regression of CVE-2019-9636 was discovered in python since commit d537ab0ff9767ef024f26246899728f0116b1ec3 affecting versions 2.7, 3.5, 3.6, 3.7 and from v3.8.0a4 through v3.8.0b1, which still allows an attacker to exploit CVE-2019-9636 by abusing the user and password parts of a URL. When an application parses user-supplied URLs to store cookies, authentication credentials, or other kind of information, it is possible for an attacker to provide specially crafted URLs to make the application locate host-related information (e.g. cookies, authentication data) and send them to a different host than where it should, unlike if the URLs had been correctly parsed. The result of an attack may vary based on the application.
CVE-2019-16056	An issue was discovered in Python through 2.7.16, 3.x through 3.5.7, 3.6.x through 3.6.9, and 3.7.x through 3.7.4. The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340
CVE-2019-16935	The documentation XML-RPC server in Python through 2.7.16, 3.x through 3.6.9, and 3.7.x through 3.7.4 has XSS via the server_title field. This occurs in Lib/DocXMLRPCServer.py in Python 2.x, and in Lib/xmlrpc/server.py in Python 3.x. If set_server_title is called with untrusted input, arbitrary JavaScript can be delivered to clients that visit the http URL for this server.
CVE-2019-9636	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.
CVE-2019-9947	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the path component of a URL that lacks a ? character) followed by an HTTP header or a Redis command. This is similar to the CVE-2019-9740 query string issue.
Samba 4.8	
CVE-2018-1050	All versions of Samba from 4.0.0 onwards are vulnerable to a denial of service attack when the RPC spoolss service is configured to be run as an external daemon. Missing input sanitization checks on some of the input parameters to spoolss RPC calls could cause the print spooler service to crash.
CVE-2018-10858	A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listing. A malicious samba server could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.
CVE-2018-10918	A null pointer dereference flaw was found in the way samba checked database outputs from the LDB database layer. An authenticated attacker could use this flaw to crash a samba server in an Active Directory Domain Controller configuration. Samba versions before 4.7.9 and 4.8.4 are vulnerable.

CVE-2018-10919	The Samba Active Directory LDAP server was vulnerable to an information disclosure flaw because of missing access control checks. An authenticated attacker could use this flaw to extract confidential attribute values using LDAP search expressions. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.
CVE-2018-1140	A missing input sanitization flaw was found in the implementation of LDP database used for the LDAP server. An attacker could use this flaw to cause a denial of service against a samba server, used as a Active Directory Domain Controller. All versions of Samba from 4.8.0 onwards are vulnerable
CVE-2018-14629	A denial of service vulnerability was discovered in Samba's LDAP server before versions 4.7.12, 4.8.7, and 4.9.3. A CNAME loop could lead to infinite recursion in the server. An unprivileged local attacker could create such an entry, leading to denial of service.
CVE-2018-16841	Samba from version 4.3.0 and before versions 4.7.12, 4.8.7 and 4.9.3 are vulnerable to a denial of service. When configured to accept smart-card authentication, Samba's KDC will call talloc_free() twice on the same memory if the principal in a validly signed certificate does not match the principal in the AS-REQ. This is only possible after authentication with a trusted certificate. talloc is robust against further corruption from a double-free with talloc_free() and directly calls abort(), terminating the KDC process.
CVE-2018-16851	Samba from version 4.0.0 and before versions 4.7.12, 4.8.7, 4.9.3 is vulnerable to a denial of service. During the processing of an LDAP search before Samba's AD DC returns the LDAP entries to the client, the entries are cached in a single memory object with a maximum size of 256MB. When this size is reached, the Samba process providing the LDAP service will follow the NULL pointer, terminating the process. There is no further vulnerability associated with this issue, merely a denial of service.
CVE-2018-16860	A flaw was found in samba's Heimdal KDC implementation, versions 4.8.x up to, excluding 4.8.12, 4.9.x up to, excluding 4.9.8 and 4.10.x up to, excluding 4.10.3, when used in AD DC mode. A man in the middle attacker could use this flaw to intercept the request to the KDC and replace the user name (principal) in the request with any desired user name (principal) that exists in the KDC effectively obtaining a ticket for that principal.
CVE-2019-3824	A flaw was found in the way an LDAP search expression could crash the shared LDAP server process of a samba AD DC in samba before version 4.10. An authenticated user, having read permissions on the LDAP server, could use this flaw to cause denial of service.
CVE-2019-3880	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.
bash 4.2.46-31.el7	
CVE-2012-6711	A heap-based buffer overflow exists in GNU Bash before 4.3 when wide characters, not supported by the current locale set in the LC_CTYPE environment variable, are printed through the echo built-in function. A local attacker, who can provide data to print through the "echo -e" built-in function, may use this flaw to crash a script or execute code with the privileges of the bash process. This occurs because ansicstr() in lib/sh/strtrans.c mishandles u32cconv().
CVE-2014-7187	Off-by-one error in the read_token_word function in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via deeply nested for loops, aka the "word_lineno" issue.

CVE-2014-7186	The redirection implementation in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via crafted use of here documents, aka the "redir_stack" issue.
CVE-2014-7169	GNU Bash through 4.3 bash43-025 processes trailing strings after certain malformed function definitions in the values of environment variables, which allows remote attackers to write to files or possibly have unknown other impact via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271.
CVE-2014-6278	GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary commands via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271, CVE-2014-7169, and CVE-2014-6277.
CVE-2014-6277	GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access, and untrusted-pointer read and write operations) via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271 and CVE-2014-7169.
CVE-2014-6271	GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.
CVE-2019-9924	rbash in Bash before 4.4-beta2 did not prevent the shell user from modifying BASH_CMDS, thus allowing the user to execute any command with the permissions of the shell.
binutils 2.27-12.el7	
CVE-2017-12448	The bfd_cache_close function in bfd/cache.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a heap use after free and possibly achieve code execution via a crafted nested archive file. This issue occurs because incorrect functions are called during an attempt to release memory. The issue can be addressed by better input validation in the bfd_generic_archive_p function in bfd/archive.c.
CVE-2017-12449	The _bfd_vms_save_sized_string function in vms-misc.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a

	crafted vms file.
CVE-2017-12450	The alpha_vms_object_p function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap write and possibly achieve code execution via a crafted vms alpha file.
CVE-2017-12451	The _bfd_xcoff_read_ar_hdr function in bfd/coff-rs6000.c and bfd/coff64-rs6000.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds stack read via a crafted COFF image file.
CVE-2017-12452	The bfd_mach_o_i386_canonicalize_one_reloc function in bfd/mach-o-i386.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted mach-o file.
CVE-2017-12453	The _bfd_vms_slurp_eeom function in libbfd.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.
CVE-2017-12454	The _bfd_vms_slurp_egsd function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an arbitrary memory read via a crafted vms alpha file.
CVE-2017-12455	The evax_bfd_print_emh function in vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.
CVE-2017-12456	The read_symbol_stabs_debugging_info function in rddbg.c in GNU Binutils 2.29 and earlier allows remote attackers to cause an out of bounds heap read via a crafted binary file.
CVE-2017-12457	The bfd_make_section_with_flags function in section.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a NULL dereference via a crafted file.
CVE-2017-12458	The nlm_swap_auxiliary_headers_in function in bfd/nlmcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted nlm file.
CVE-2017-12459	The bfd_mach_o_read_symtab_strtab function in bfd/mach-o.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap write and possibly achieve code execution via a crafted mach-o file.
CVE-2017-12799	The elf_read_notesfunction in bfd/elf.c in GNU Binutils 2.29 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file.
CVE-2019-1010204	GNU binutils gold gold v1.11-v1.16 (GNU binutils v2.21-v2.31.1) is affected by: Improper Input Validation, Signed/Unsigned Comparison, Out-of-bounds Read. The impact is: Denial of service. The component is: gold/fileread.cc:497, elfcpp/elfcpp_file.h:644. The attack vector is: An ELF file with an invalid e_shoff header field must be opened.
cmake 2.8.12.2-2.el7	
	None
coreutils 8.22-23.el7	
	None
cryptsetup 2.0.3-3.el7	
CVE-2016-4484	The Debian initrd script for the cryptsetup package 2:1.7.3-2 and earlier allows physically proximate attackers to gain shell access via many log in attempts with an invalid password.

curl 7.29.0-51.el7_6.3	
CVE-2013-1944	The tailMatch function in cookie.c in cURL and libcurl before 7.30.0 does not properly match the path domain when sending cookies, which allows remote attackers to steal cookies via a matching suffix in the domain of a URL.
CVE-2013-2174	Heap-based buffer overflow in the curl_easy_unescape function in lib/escape.c in cURL and libcurl 7.7 through 7.30.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string ending in a "%" (percent) character.
CVE-2013-4545	cURL and libcurl 7.18.0 through 7.32.0, when built with OpenSSL, disables the certificate CN and SAN name field verification (CURLOPT_SSL_VERIFYHOST) when the digital signature verification (CURLOPT_SSL_VERIFYPEER) is disabled, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.
CVE-2014-0015	cURL and libcurl 7.10.6 through 7.34.0, when more than one authentication method is enabled, re-uses NTLM connections, which might allow context-dependent attackers to authenticate as other users via a request.
CVE-2014-0138	The default configuration in cURL and libcurl 7.10.6 before 7.36.0 re-uses (1) SCP, (2) SFTP, (3) POP3, (4) POP3S, (5) IMAP, (6) IMAPS, (7) SMTP, (8) SMTPS, (9) LDAP, and (10) LDAPS connections, which might allow context-dependent attackers to connect as other users via a request, a similar issue to CVE-2014-0015.
CVE-2014-0139	cURL and libcurl 7.1 before 7.36.0, when using the OpenSSL, axtls, qsossl or gskit libraries for TLS, recognize a wildcard IP address in the subject's Common Name (CN) field of an X.509 certificate, which might allow man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.
CVE-2014-2522	curl and libcurl 7.27.0 through 7.35.0, when running on Windows and using the SChannel/Winssl TLS backend, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate when accessing a URL that uses a numerical IP address, which allows man-in-the-middle attackers to spoof servers via an arbitrary valid certificate.
CVE-2015-3143	cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use NTLM connections, which allows remote attackers to connect as other users via an unauthenticated request, a similar issue to CVE-2014-0015.
CVE-2015-3148	cURL and libcurl 7.10.6 through 7.41.0 do not properly re-use authenticated Negotiate connections, which allows remote attackers to connect as other users via a request.
CVE-2016-0754	cURL before 7.47.0 on Windows allows attackers to write to arbitrary files in the current working directory on a different drive via a colon in a remote file name.
CVE-2016-3739	The (1) mbed_connect_step1 function in lib/vtls/mbedtls.c and (2) polarssl_connect_step1 function in lib/vtls/polarssl.c in cURL and libcurl before 7.49.0, when using SSLv3 or making a TLS connection to a URL that uses a numerical IP address, allow remote attackers to spoof servers via an arbitrary valid certificate.
CVE-2016-4802	Multiple untrusted search path vulnerabilities in cURL and libcurl before 7.49.1, when built with SSPI or telnet is enabled, allow local users to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse (1) security.dll, (2) secur32.dll, or (3) ws2_32.dll in the application or current working directory.
CVE-2016-5419	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed, which allows remote attackers to bypass intended restrictions by resuming a session.
CVE-2016-5420	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, which might allow remote attackers to hijack the

	authentication of the connection by leveraging a previously created connection with a different client certificate.
CVE-2016-7141	curl and libcurl before 7.50.2, when built with NSS and the libnsspem.so library is available at runtime, allow remote attackers to hijack the authentication of a TLS connection by leveraging reuse of a previously loaded client certificate from file for a connection for which no certificate has been set, a different vulnerability than CVE-2016-5420.
CVE-2016-7167	Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape, (3) curl_unescape, and (4) curl_easy_unescape functions in libcurl before 7.50.3 allow attackers to have unspecified impact via a string of length 0xffffffff, which triggers a heap-based buffer overflow.
CVE-2016-8615	A flaw was found in curl before version 7.51. If cookie state is written into a cookie jar file that is later read back and used for subsequent requests, a malicious HTTP server can inject new cookies for arbitrary domains into said cookie jar.
CVE-2016-8616	A flaw was found in curl before version 7.51.0 When re-using a connection, curl was doing case insensitive comparisons of user name and password with the existing connections. This means that if an unused connection with proper credentials exists for a protocol that has connection-scoped credentials, an attacker can cause that connection to be reused if s/he knows the case-insensitive version of the correct password.
CVE-2016-8617	The base64 encode function in curl before version 7.51.0 is prone to a buffer being under allocated in 32bit systems if it receives at least 1Gb as input via `CURLOPT_USERNAME`.
CVE-2016-8618	The libcurl API function called `curl_maprintf()` before version 7.51.0 can be tricked into doing a double-free due to an unsafe `size_t` multiplication, on systems using 32 bit `size_t` variables.
CVE-2016-8619	The function `read_data()` in security.c in curl before version 7.51.0 is vulnerable to memory double free.
CVE-2016-8620	The 'globbing' feature in curl before version 7.51.0 has a flaw that leads to integer overflow and out-of-bounds read via user controlled input.
CVE-2016-8621	The `curl_getdate` function in curl before version 7.51.0 is vulnerable to an out of bounds read if it receives an input with one digit short.
CVE-2016-8622	The URL percent-encoding decode function in libcurl before 7.51.0 is called `curl_easy_unescape`. Internally, even if this function would be made to allocate a unscape destination buffer larger than 2GB, it would return that new length in a signed 32 bit integer variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer.
CVE-2016-8623	A flaw was found in curl before version 7.51.0. The way curl handles cookies permits other threads to trigger a use-after-free leading to information disclosure.
CVE-2016-8624	curl before version 7.51.0 doesn't parse the authority component of the URL correctly when the host name part ends with a '#' character, and could instead be tricked into connecting to a different host. This may have security implications if you for example use an URL parser that follows the RFC to check for allowed domains before using curl to request them.
CVE-2016-8625	curl before version 7.51.0 uses outdated IDNA 2003 standard to handle International Domain Names and this may lead users to potentially and unknowingly issue network transfer requests to the wrong host.
CVE-2016-9586	curl before version 7.52.0 is vulnerable to a buffer overflow when doing a large floating point output in libcurl's implementation of the printf() functions. If there are any application that accepts a format string from the outside without necessary input filtering, it could allow remote attacks.
CVE-2016-9594	curl before version 7.52.1 is vulnerable to an uninitialized random in libcurl's

	internal function that returns a good 32bit random value. Having a weak or virtually non-existent random value makes the operations that use it vulnerable.
CVE-2017-2629	curl before 7.53.0 has an incorrect TLS Certificate Status Request extension feature that asks for a fresh proof of the server's certificate's validity in the code that checks for a test success or failure. It ends up always thinking there's valid proof, even when there is none or if the server doesn't support the TLS extension in question. This could lead to users not detecting when a server's certificate goes invalid or otherwise be misleading that the server is in a better shape than it is in reality. This flaw also exists in the command line tool (–cert-status).
CVE-2017-8816	The NTLM authentication feature in curl and libcurl before 7.57.0 on 32-bit platforms allows attackers to cause a denial of service (integer overflow and resultant buffer overflow, and application crash) or possibly have unspecified other impact via vectors involving long user and password fields.
CVE-2017-8817	The FTP wildcard function in curl and libcurl before 7.57.0 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) or possibly have unspecified other impact via a string that ends with an '[' character.
CVE-2017-8818	curl and libcurl before 7.57.0 on 32-bit platforms allow attackers to cause a denial of service (out-of-bounds access and application crash) or possibly have unspecified other impact because too little memory is allocated for interfacing to an SSL library.
CVE-2018-1000007	libcurl 7.1 through 7.57.0 might accidentally leak authentication data to third parties. When asked to send custom headers in its HTTP requests, libcurl will send that set of headers first to the host in the initial URL but also, if asked to follow redirects and a 30X HTTP response code is returned, to the host mentioned in URL in the `Location:` response header value. Sending the same set of headers to subsequent hosts is in particular a problem for applications that pass on custom `Authorization:` headers, as this header often contains privacy sensitive information or data that could allow others to impersonate the libcurl-using client's request.
CVE-2018-1000120	A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL handling that allows an attacker to cause a denial of service or worse.
CVE-2018-1000121	A NULL pointer dereference exists in curl 7.21.0 to and including curl 7.58.0 in the LDAP code that allows an attacker to cause a denial of service
CVE-2018-1000122	A buffer over-read exists in curl 7.20.0 to and including curl 7.58.0 in the RTSP+RTP handling code that allows an attacker to cause a denial of service or information leakage
CVE-2018-1000301	curl version curl 7.20.0 to and including curl 7.59.0 contains a CWE-126: Buffer Over-read vulnerability in denial of service that can result in curl can be tricked into reading data beyond the end of a heap based buffer used to store downloaded RTSP content.. This vulnerability appears to have been fixed in curl < 7.20.0 and curl >= 7.60.0.
CVE-2018-14618	curl before version 7.61.1 is vulnerable to a buffer overrun in the NTLM authentication code. The internal function Curl_ntlm_core_mk_nt_hash multiplies the length of the password by two (SUM) to figure out how large temporary storage area to allocate from the heap. The length value is then subsequently used to iterate over the password and generate output into the allocated storage buffer. On systems with a 32 bit size_t, the math to calculate SUM triggers an integer overflow when the password length exceeds 2GB (2^31 bytes). This integer overflow usually causes a very small buffer to actually get allocated instead of the intended very huge one, making the use of that buffer end up in a heap buffer overflow. (This bug is almost identical to CVE-2017-8816.)

CVE-2018-16842	Curl versions 7.14.1 through 7.61.1 are vulnerable to a heap-based buffer over-read in the tool_msgs.c:voutf() function that may result in information exposure and denial of service.
CVE-2019-5436	A heap buffer overflow in the TFTP receiving code allows for DoS or arbitrary code execution in libcurl versions 7.19.4 through 7.64.1.
CVE-2019-5443	A non-privileged user or program can put code and a config file in a known non-privileged path (under C:/usr/local/) that will make curl <= 7.65.1 automatically run the code (as an openssl "engine") on invocation. If that curl is invoked by a privileged user it can do anything it wants.
CVE-2019-5482	Heap buffer overflow in the TFTP protocol handler in cURL 7.19.4 to 7.65.3.
dbus 1.10.24-13.el7_6	
	None
dhclient 4.2.5-68.el7.1	
CVE-2018-5732	Failure to properly bounds-check a buffer used for processing DHCP options allows a malicious server (or an entity masquerading as a server) to cause a buffer overflow (and resulting crash) in dhclient by sending a response containing a specially constructed options section. Affects ISC DHCP versions 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0
docker-ce 19.03.1-3.el7	
	None
dosfstools 3.0.20-10.el7	
CVE-2015-8872	The set_fat function in fat.c in dosfstools before 4.0 might allow attackers to corrupt a FAT12 filesystem or cause a denial of service (invalid memory read and crash) by writing an odd number of clusters to the third to last entry on a FAT12 filesystem, which triggers an "off-by-two error."
CVE-2016-4804	The read_boot function in boot.c in dosfstools before 4.0 allows attackers to cause a denial of service (crash) via a crafted filesystem, which triggers a heap-based buffer overflow in the (1) read_fat function or an out-of-bounds heap read in (2) get_fat function.
dracut 033-554.el7	
CVE-2016-8637	A local information disclosure issue was found in dracut before 045 when generating initramfs images with world-readable permissions when 'early cpio' is used, such as when including microcode updates. Local attacker can use this to obtain sensitive information from these files, such as encryption keys or credentials.
elfutils 0.172-2.el7	
CVE-2018-16062	dwarf_getaranges in dwarf_getaranges.c in libdw in elfutils before 2018-08-18 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted file.
ethtool 4.8-9.el7	
	None
firewalld 0.5.3-5.el7	
	None
freetype 2.8-12.el7_6.1	
CVE-2018-6942	An issue was discovered in FreeType 2 through 2.9. A NULL pointer dereference in the Ins_GETVARIATION() function within ttinterp.c could lead to DoS via a crafted font file.
glibc 2.17-260.el7_6.6	
CVE-2012-4412	Integer overflow in string/strcoll_l.c in the GNU C Library (aka glibc or libc6) 2.17 and earlier allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a heap-based buffer overflow.
CVE-2012-4424	Stack-based buffer overflow in string/strcoll_l.c in the GNU C Library (aka glibc or libc6) 2.17 and earlier allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string that

	triggers a malloc failure and use of the alloca function.
CVE-2013-0242	Buffer overflow in the extend_buffers function in the regular expression matcher (posix/regexec.c) in glibc, possibly 2.17 and earlier, allows context-dependent attackers to cause a denial of service (memory corruption and crash) via crafted multibyte characters.
CVE-2013-1914	Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in GNU C Library (aka glibc or libc6) 2.17 and earlier allows remote attackers to cause a denial of service (crash) via a (1) hostname or (2) IP address that triggers a large number of domain conversion results.
CVE-2013-2207	pt_chown in GNU C Library (aka glibc or libc6) before 2.18 does not properly check permissions for tty files, which allows local users to change the permission on the files and obtain access to arbitrary pseudo-terminals by leveraging a FUSE file system.
CVE-2013-4237	sysdeps/posix/readdir_r.c in the GNU C Library (aka glibc or libc6) 2.18 and earlier allows context-dependent attackers to cause a denial of service (out-of-bounds write and crash) or possibly execute arbitrary code via a crafted (1) NTFS or (2) CIFS image.
CVE-2013-4332	Multiple integer overflows in malloc/malloc.c in the GNU C Library (aka glibc or libc6) 2.18 and earlier allow context-dependent attackers to cause a denial of service (heap corruption) via a large value to the (1) pvalloc, (2) valloc, (3) posix_memalign, (4) memalign, or (5) aligned_alloc functions.
CVE-2013-4458	Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in GNU C Library (aka glibc or libc6) 2.18 and earlier allows remote attackers to cause a denial of service (crash) via a (1) hostname or (2) IP address that triggers a large number of AF_INET6 address results. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-1914.
CVE-2013-4788	The PTR_MANGLE implementation in the GNU C Library (aka glibc or libc6) 2.4, 2.17, and earlier, and Embedded GLIBC (EGLIBC) does not initialize the random value for the pointer guard, which makes it easier for context-dependent attackers to control execution flow by leveraging a buffer-overflow vulnerability in an application and using the known zero value pointer guard to calculate a pointer address.
CVE-2013-7423	The send_dg function in resolv/res_send.c in GNU C Library (aka glibc or libc6) before 2.20 does not properly reuse file descriptors, which allows remote attackers to send DNS queries to unintended locations via a large number of requests that trigger a call to the getaddrinfo function.
CVE-2014-0475	Multiple directory traversal vulnerabilities in GNU C Library (aka glibc or libc6) before 2.20 allow context-dependent attackers to bypass ForceCommand restrictions and possibly have other unspecified impact via a .. (dot dot) in a (1) LC_*, (2) LANG, or other locale environment variable.
CVE-2014-6040	GNU C Library (aka glibc) before 2.20 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via a multibyte character value of "0xffff" to the iconv function when converting (1) IBM933, (2) IBM935, (3) IBM937, (4) IBM939, or (5) IBM1364 encoded data to UTF-8.
CVE-2015-0235	Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostbyname2 function, aka "GHOST."
CVE-2015-7547	Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family,

	related to performing "dual A/AAAA DNS queries" and the libnss_dns.so.2 NSS module.
CVE-2016-10228	The iconv program in the GNU C Library (aka glibc or libc6) 2.25 and earlier, when invoked with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.
CVE-2016-10739	In the GNU C Library (aka glibc or libc6) through 2.28, the getaddrinfo function would successfully parse a string that contained an IPv4 address followed by whitespace and arbitrary characters, which could lead applications to incorrectly assume that it had parsed a valid string, without the possibility of embedded HTTP headers or other potentially dangerous substrings.
CVE-2016-1234	Stack-based buffer overflow in the glob implementation in GNU C Library (aka glibc) before 2.24, when GLOB_ALTDIRFUNC is used, allows context-dependent attackers to cause a denial of service (crash) via a long name.
CVE-2016-3075	Stack-based buffer overflow in the nss_dns implementation of the getnetbyname function in GNU C Library (aka glibc) before 2.24 allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a long name.
CVE-2017-12132	The DNS stub resolver in the GNU C Library (aka glibc or libc6) before version 2.26, when EDNS support is enabled, will solicit large UDP responses from name servers, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation.
CVE-2017-12133	Use-after-free vulnerability in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) before 2.26 allows remote attackers to have unspecified impact via vectors related to error path.
CVE-2017-15670	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buffer overflow in the glob function in glob.c, related to the processing of home directories using the ~ operator followed by a long string.
CVE-2017-15671	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27, when invoked with GLOB_TILDE, could skip freeing allocated memory when processing the ~ operator with a long user name, potentially leading to a denial of service (memory leak).
CVE-2017-15804	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator.
CVE-2018-1000001	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.
CVE-2018-11236	stdlib/canonicalize.c in the GNU C Library (aka glibc or libc6) 2.27 and earlier, when processing very long pathname arguments to the realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffer overflow and, potentially, arbitrary code execution.
CVE-2018-11237	An AVX-512-optimized implementation of the mempcpy function in the GNU C Library (aka glibc or libc6) 2.27 and earlier may write data beyond the target buffer, leading to a buffer overflow in __mempcpy_avx512_no_vzeroupper.
CVE-2018-19591	In the GNU C Library (aka glibc or libc6) through 2.28, attempting to resolve a crafted hostname via getaddrinfo() leads to the allocation of a socket descriptor that is not closed. This is related to the if_nametoindex() function.
CVE-2018-20796	In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.
CVE-2018-6485	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.

CVE-2019-6488	The string component in the GNU C Library (aka glibc or libc6) through 2.28, when running on the x32 architecture, incorrectly attempts to use a 64-bit register for size_t in assembly codes, which can lead to a segmentation fault or possibly unspecified other impact, as demonstrated by a crash in __memmove_avx_unaligned_erms in sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S during a memcpy.
CVE-2019-7309	In the GNU C Library (aka glibc or libc6) through 2.29, the memcmp function for the x32 architecture can incorrectly return zero (indicating that the inputs are equal) because the RDX most significant bit is mishandled.
CVE-2019-9169	In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer over-read via an attempted case-insensitive regular-expression match.
CVE-2019-9192	** In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern.
graphicsmagick 1.3.31-2.el7	
CVE-2018-20189	In GraphicsMagick 1.3.31, the ReadDIBImage function of coders/dib.c has a vulnerability allowing a crash and denial of service via a dib file that is crafted to appear with direct pixel values and also colormapping (which is not available beyond 8-bits/sample), and therefore lacks indexes initialization.
CVE-2019-11005	In GraphicsMagick 1.4 snapshot-20190322 Q8, there is a stack-based buffer overflow in the function SVGStartElement of coders/svg.c, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a quoted font family value.
CVE-2019-11006	In GraphicsMagick 1.4 snapshot-20190322 Q8, there is a heap-based buffer over-read in the function ReadMIFFImage of coders/miff.c, which allows attackers to cause a denial of service or information disclosure via an RLE packet.
CVE-2019-11007	In GraphicsMagick 1.4 snapshot-20190322 Q8, there is a heap-based buffer over-read in the ReadMNGImage function of coders/png.c, which allows attackers to cause a denial of service or information disclosure via an image colormap.
CVE-2019-11008	In GraphicsMagick 1.4 snapshot-20190322 Q8, there is a heap-based buffer overflow in the function WriteXWDImage of coders/xwd.c, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image file.
CVE-2019-11009	In GraphicsMagick 1.4 snapshot-20190322 Q8, there is a heap-based buffer over-read in the function ReadXWDImage of coders/xwd.c, which allows attackers to cause a denial of service or information disclosure via a crafted image file.
CVE-2019-11010	In GraphicsMagick 1.4 snapshot-20190322 Q8, there is a memory leak in the function ReadMPCImage of coders/mpc.c, which allows attackers to cause a denial of service via a crafted image file.
CVE-2019-11473	coders/xwd.c in GraphicsMagick 1.3.31 allows attackers to cause a denial of service (out-of-bounds read and application crash) by crafting an XWD image file, a different vulnerability than CVE-2019-11008 and CVE-2019-11009.
CVE-2019-11474	coders/xwd.c in GraphicsMagick 1.3.31 allows attackers to cause a denial of service (floating-point exception and application crash) by crafting an XWD image file, a different vulnerability than CVE-2019-11008 and CVE-2019-11009.
CVE-2019-11505	In GraphicsMagick from version 1.3.8 to 1.4 snapshot-20190403 Q8, there is a heap-based buffer overflow in the function WritePDBImage of coders/pdb.c, which allows an attacker to cause a denial of service or possibly have

	unspecified other impact via a crafted image file. This is related to MagickBitStreamMSBWrite in magick/bit_stream.c.
CVE-2019-11506	In GraphicsMagick from version 1.3.30 to 1.4 snapshot-20190403 Q8, there is a heap-based buffer overflow in the function WriteMATLABImage of coders/mat.c, which allows an attacker to cause a denial of service or possibly have unspecified other impact via a crafted image file. This is related to ExportRedQuantumType in magick/export.c.
CVE-2019-7397	In ImageMagick before 7.0.8-25 and GraphicsMagick through 1.3.31, several memory leaks exist in WritePDFImage in coders/pdf.c.
haproxy 1.5.18-8.el7	
CVE-2019-11323	HAProxy before 1.9.7 mishandles a reload with rotated keys, which triggers use of uninitialized, and very predictable, HMAC keys. This is related to an include/types/ssl_sock.h error.
CVE-2019-14241	HAProxy through 2.0.2 allows attackers to cause a denial of service (ha_panic) via vectors related to htx_manage_client_side_cookies in proto_htx.c.
imagemagick 6.7.8.9-15.el7_2	
CVE-2015-8900	The ReadHDRImage function in coders/hdr.c in ImageMagick 6.x and 7.x allows remote attackers to cause a denial of service (infinite loop) via a crafted HDR file.
CVE-2015-8901	ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted MIFF file.
CVE-2015-8902	The ReadBlobByte function in coders/pdb.c in ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted PDB file.
CVE-2015-8903	The ReadVICARImage function in coders/vicar.c in ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted VICAR file.
CVE-2017-17499	ImageMagick before 6.9.9-24 and 7.x before 7.0.7-12 has a use-after-free in Magick::Image::read in Magick++/lib/Image.cpp.
CVE-2017-17504	ImageMagick before 7.0.7-12 has a coders/png.c Magick_png_read_raw_profile heap-based buffer over-read via a crafted file, related to ReadOneMNGImage.
CVE-2018-16323	ReadXBMImage in coders/xbm.c in ImageMagick before 7.0.8-9 leaves data uninitialized when processing an XBM file that has a negative pixel value. If the affected code is used as a library loaded into a process that includes sensitive information, that information sometimes can be leaked via the image data.
CVE-2018-16328	In ImageMagick before 7.0.8-8, a NULL pointer dereference exists in the CheckEventLogging function in MagickCore/log.c.
CVE-2018-16329	In ImageMagick before 7.0.8-8, a NULL pointer dereference exists in the GetMagickProperty function in MagickCore/property.c.
CVE-2018-20467	In coders/bmp.c in ImageMagick before 7.0.8-16, an input file can result in an infinite loop and hang, with high CPU and memory consumption. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted file.
CVE-2018-6405	In the ReadDCMImage function in coders/dcm.c in ImageMagick before 7.0.7-23, each redmap, greenmap, and bluemap variable can be overwritten by a new pointer. The previous pointer is lost, which leads to a memory leak. This allows remote attackers to cause a denial of service.
CVE-2019-10131	An off-by-one read vulnerability was discovered in ImageMagick before version 7.0.7-28 in the formatIPTCfromBuffer function in coders/meta.c. A local attacker may use this flaw to read beyond the end of the buffer or to crash the program.
CVE-2019-10714	LocaleLowercase in MagickCore/locale.c in ImageMagick before 7.0.8-32 allows out-of-bounds access, leading to a SIGSEGV.
CVE-2019-13133	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function

	ReadBMPImage in coders/bmp.c.
CVE-2019-13134	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadVIFFImage in coders/viff.c.
CVE-2019-13135	ImageMagick before 7.0.8-50 has a "use of uninitialized value" vulnerability in the function ReadCUTImage in coders/cut.c.
CVE-2019-13136	ImageMagick before 7.0.8-50 has an integer overflow vulnerability in the function TIFFSeekCustomStream in coders/tiff.c.
CVE-2019-13137	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadPSImage in coders/ps.c.
CVE-2019-14980	In ImageMagick 7.x before 7.0.8-42 and 6.x before 6.9.10-42, there is a use after free vulnerability in the UnmapBlob function that allows an attacker to cause a denial of service by sending a crafted file.
CVE-2019-14981	In ImageMagick 7.x before 7.0.8-41 and 6.x before 6.9.10-41, there is a divide-by-zero vulnerability in the MeanShiftImage function. It allows an attacker to cause a denial of service by sending a crafted file.
CVE-2019-7175	In ImageMagick before 7.0.8-25, some memory leaks exist in DecodeImage in coders/pcd.c.
CVE-2019-7395	In ImageMagick before 7.0.8-25, a memory leak exists in WritePSDChannel in coders/psd.c.
CVE-2019-7396	In ImageMagick before 7.0.8-25, a memory leak exists in ReadSIXELImage in coders/sixel.c.
CVE-2019-7397	In ImageMagick before 7.0.8-25 and GraphicsMagick through 1.3.31, several memory leaks exist in WritePDFImage in coders/pdf.c.
CVE-2019-7398	In ImageMagick before 7.0.8-25, a memory leak exists in WriteDIBImage in coders/dib.c.
iproute 4.11.0-14.el7_6.2	
	None
iptables 1.4.21-28.el7	
CVE-2012-2663	extensions/libxt_tcp.c in iptables through 1.4.21 does not match TCP SYN+FIN packets in --syn rules, which might allow remote attackers to bypass intended firewall restrictions via crafted packets. NOTE: the CVE-2012-6638 fix makes this issue less relevant.
java openjdk 1.8.0.181-7.b13.el7	
CVE-2012-2739	Oracle Java SE before 7 Update 6, and OpenJDK 7 before 7u6 build 12 and 8 before build 39, computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table.
CVE-2013-0169	The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.
CVE-2014-1876	The unpacker::redirect_stdio function in unpack.cpp in unpack200 in OpenJDK 6, 7, and 8
jq 1.5-1.el7	
CVE-2015-8863	Off-by-one error in the tokenadd function in jv_parse.c in jq allows remote attackers to cause a denial of service (crash) via a long JSON-encoded number, which triggers a heap-based buffer overflow.
CVE-2016-4074	The jv_dump_term function in jq 1.5 allows remote attackers to cause a denial of service (stack consumption and application crash) via a crafted JSON file.
kbd 1.15.5-15.el7	
	None
keyutils 1.5.8-3.el7	

	None
kubectl 1.14.1-0	
CVE-2019-11244	In Kubernetes v1.8.x-v1.14.x, schema info is cached by kubectl in the location specified by --cache-dir (defaulting to $HOME/.kube/http-cache), written with world-writeable permissions (rw-rw-rw-). If --cache-dir is specified and pointed at a different location accessible to other users/groups, the written files may be modified by other users/groups and disrupt the kubectl invocation.
CVE-2019-11246	The kubectl cp command allows copying files between containers and the user machine. To copy files from a container, Kubernetes runs tar inside the container to create a tar archive, copies it over the network, and kubectl unpacks it on the user&#8217
CVE-2019-11249	The kubectl cp command allows copying files between containers and the user machine. To copy files from a container, Kubernetes runs tar inside the container to create a tar archive, copies it over the network, and kubectl unpacks it on the user&#8217
kubelet 1.14.1-0	
CVE-2019-11248	The debugging endpoint /debug/pprof is exposed over the unauthenticated Kubelet healthz port. The go pprof endpoint is exposed over the Kubelet's healthz port. This debugging endpoint can potentially leak sensitive information such as internal Kubelet memory addresses and configuration, or for limited denial of service. Versions prior to 1.15.0, 1.14.4, 1.13.8, and 1.12.10 are affected. The issue is of medium severity, but not exposed by the default configuration.
libarchive 3.1.2-10.el7_2	
CVE-2018-1000877	libarchive version commit 416694915449219d505531b1096384f3237dd6cc onwards (release v3.1.0 onwards) contains a CWE-415: Double Free vulnerability in RAR decoder - libarchive/archive_read_support_format_rar.c, parse_codes(), realloc(rar->lzss.window, new_size) with new_size = 0 that can result in Crash/DoS. This attack appear to be exploitable via the victim must open a specially crafted RAR archive.
CVE-2018-1000878	libarchive version commit 416694915449219d505531b1096384f3237dd6cc onwards (release v3.1.0 onwards) contains a CWE-416: Use After Free vulnerability in RAR decoder - libarchive/archive_read_support_format_rar.c that can result in Crash/DoS - it is unknown if RCE is possible. This attack appear to be exploitable via the victim must open a specially crafted RAR archive.
CVE-2019-1000019	libarchive version commit bf9aec176c6748f0ee7a678c5f9f9555b9a757c1 onwards (release v3.0.2 onwards) contains a CWE-125: Out-of-bounds Read vulnerability in 7zip decompression, archive_read_support_format_7zip.c, header_bytes() that can result in a crash (denial of service). This attack appears to be exploitable via the victim opening a specially crafted 7zip file.
CVE-2019-1000020	libarchive version commit 5a98dcf8a86364b3c2c469c85b93647dfb139961 onwards (version v2.8.0 onwards) contains a CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in ISO9660 parser, archive_read_support_format_iso9660.c, read_CE()/parse_rockridge() that can result in DoS by infinite loop. This attack appears to be exploitable via the victim opening a specially crafted ISO9660 file.
libcgroup 0.41-20.el7	
CVE-2018-14348	libcgroup up to and including 0.41 creates /var/log/cgred with mode 0666 regardless of the configured umask, leading to disclosure of information.
libcroco 0.6.12-4.el7	
CVE-2017-7960	The cr_input_new_from_uri function in cr-input.c in libcroco 0.6.11 and 0.6.12 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted CSS file.
CVE-2017-7961	** The cr_tknzr_parse_rgb function in cr-tknzr.c in libcroco 0.6.11 and 0.6.12

	has an "outside the range of representable values of type long" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted CSS file. NOTE: third-party analysis reports "This is not a security issue in my view. The conversion surely is truncating the double into a long value, but there is no impact as the value is one of the RGB components."
CVE-2017-8834	The cr_tknzr_parse_comment function in cr-tknzr.c in libcroco 0.6.12 allows remote attackers to cause a denial of service (memory allocation error) via a crafted CSS file.
CVE-2017-8871	The cr_parser_parse_selector_core function in cr-parser.c in libcroco 0.6.12 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted CSS file.
libcurl 7.29.0-51.el7_6.3	
CVE-2013-1944	The tailMatch function in cookie.c in cURL and libcurl before 7.30.0 does not properly match the path domain when sending cookies, which allows remote attackers to steal cookies via a matching suffix in the domain of a URL.
CVE-2013-2174	Heap-based buffer overflow in the curl_easy_unescape function in lib/escape.c in cURL and libcurl 7.7 through 7.30.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string ending in a "%" (percent) character.
CVE-2013-4545	cURL and libcurl 7.18.0 through 7.32.0, when built with OpenSSL, disables the certificate CN and SAN name field verification (CURLOPT_SSL_VERIFYHOST) when the digital signature verification (CURLOPT_SSL_VERIFYPEER) is disabled, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.
CVE-2013-6422	The GnuTLS backend in libcurl 7.21.4 through 7.33.0, when disabling digital signature verification (CURLOPT_SSL_VERIFYPEER), also disables the CURLOPT_SSL_VERIFYHOST check for CN or SAN host name fields, which makes it easier for remote attackers to spoof servers and conduct man-in-the-middle (MITM) attacks.
CVE-2014-0015	cURL and libcurl 7.10.6 through 7.34.0, when more than one authentication method is enabled, re-uses NTLM connections, which might allow context-dependent attackers to authenticate as other users via a request.
CVE-2014-0138	The default configuration in cURL and libcurl 7.10.6 before 7.36.0 re-uses (1) SCP, (2) SFTP, (3) POP3, (4) POP3S, (5) IMAP, (6) IMAPS, (7) SMTP, (8) SMTPS, (9) LDAP, and (10) LDAPS connections, which might allow context-dependent attackers to connect as other users via a request, a similar issue to CVE-2014-0.
CVE-2014-0139	cURL and libcurl 7.1 before 7.36.0, when using the OpenSSL, axtls, qsossl or gskit libraries for TLS, recognize a wildcard IP address in the subject's Common Name (CN) field of an X.509 certificate, which might allow man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.
CVE-2014-2522	curl and libcurl 7.27.0 through 7.35.0, when running on Windows and using the SChannel/Winssl TLS backend, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate when accessing a URL that uses a numerical IP address, which allows man-in-the-middle attackers to spoof servers via an arbitrary valid certificate.
CVE-2014-3707	The curl_easy_duphandle function in libcurl 7.17.1 through 7.38.0, when running with the CURLOPT_COPYPOSTFIELDS option, does not properly copy HTTP POST data for an easy handle, which triggers an out-of-bounds read that allows remote web servers to read sensitive memory information.
CVE-2014-8150	CRLF injection vulnerability in libcurl 6.0 through 7.x before 7.40.0, when using an HTTP proxy, allows remote attackers to inject arbitrary HTTP headers and

	conduct HTTP response splitting attacks via CRLF sequences in a URL.
CVE-2015-3143	cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use NTLM connections, which allows remote attackers to connect as other users via an unauthenticated request, a similar issue to CVE-2014-0.
CVE-2015-3148	cURL and libcurl 7.10.6 through 7.41.0 do not properly re-use authenticated Negotiate connections, which allows remote attackers to connect as other users via a request.
CVE-2016-8622	The URL percent-encoding decode function in libcurl before 7.51.0 is called \`curl_easy_unescape\`. Internally, even if this function would be made to allocate a unscape destination buffer larger than 2GB, it would return that new length in a signed 32 bit integer variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer.
CVE-2017-1000257	An IMAP FETCH response line indicates the size of the returned data, in number of bytes. When that response says the data is zero bytes, libcurl would pass on that (non-existing) data with a pointer and the size (zero) to the deliver-data function. libcurl's deliver-data function treats zero as a magic number and invokes strlen() on the data to figure out the length. The strlen() is called on a heap based buffer that might not be zero terminated so libcurl might read beyond the end of it into whatever memory lies after (or just crash) and then deliver that to the application as if it was actually downloaded.
CVE-2019-5436	A heap buffer overflow in the TFTP receiving code allows for DoS or arbitrary code execution in libcurl versions 7.19.4 through 7.64.1.
libpcap 1.5.3-11.el7	
CVE-2018-16301	libpcap before 1.9.1, as used in tcpdump before 4.9.3, has a buffer overflow and/or over-read because of errors in pcapng reading.
CVE-2019-15161	rpcapd/daemon.c in libpcap before 1.9.1 mishandles certain length values because of reuse of a variable. This may open up an attack vector involving extra data at the end of a request.
CVE-2019-15162	rpcapd/daemon.c in libpcap before 1.9.1 on non-Windows platforms provides details about why authentication failed, which might make it easier for attackers to enumerate valid usernames.
CVE-2019-15163	rpcapd/daemon.c in libpcap before 1.9.1 allows attackers to cause a denial of service (NULL pointer dereference and daemon crash) if a crypt() call fails.
CVE-2019-15164	rpcapd/daemon.c in libpcap before 1.9.1 allows SSRF because a URL may be provided as a capture source.
CVE-2019-15165	sf-pcapng.c in libpcap before 1.9.1 does not properly validate the PHB header length before allocating memory.
libpng 1.5.13-7.el7_2	
CVE-2013-7353	Integer overflow in the png_set_unknown_chunks function in libpng/pngset.c in libpng before 1.5.14beta08 allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a crafted image, which triggers a heap-based buffer overflow.
CVE-2013-7354	Multiple integer overflows in libpng before 1.5.14rc03 allow remote attackers to cause a denial of service (crash) via a crafted image to the (1) png_set_sPLT or (2) png_set_text_2 function, which triggers a heap-based buffer overflow.
CVE-2015-8472	Buffer overflow in the png_set_PLTE function in libpng before 1.0.65, 1.1.x and 1.2.x before 1.2.55, 1.3.x, 1.4.x before 1.4.18, 1.5.x before 1.5.25, and 1.6.x before 1.6.20 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a small bit-depth value in an IHDR (aka image header) chunk in a PNG image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2-8126.
CVE-2015-8540	Integer underflow in the png_check_keyword function in pngwutil.c in libpng 0.90 through 0.99, 1.0.x before 1.0.66, 1.1.x and 1.2.x before 1.2.56, 1.3.x and 1.4.x before 1.4.19, and 1.5.x before 1.5.26 allows remote attackers to have

	unspecified impact via a space character as a keyword in a PNG image, which triggers an out-of-bounds read.
CVE-2016-10087	The png_set_text_2 function in libpng 0.71 before 1.0.67, 1.2.x before 1.2.57, 1.4.x before 1.4.20, 1.5.x before 1.5.28, and 1.6.x before 1.6.27 allows context-dependent attackers to cause a NULL pointer dereference vectors involving loading a text chunk into a png structure, removing the text, and then adding another text chunk to the structure.
CVE-2017-12652	libpng before 1.6.32 does not properly check the length of chunks against the user limit.
libseccomp 2.3.1-3.el7	
CVE-2019-9893	libseccomp before 2.4.0 did not correctly generate 64-bit syscall argument comparisons using the arithmetic operators (LT, GT, LE, GE), which might able to lead to bypassing seccomp filters and potential privilege escalations.
libssh2 1.4.3-12.el7_6.3	
CVE-2015-1782	The kex_agree_methods function in libssh2 before 1.5.0 allows remote servers to cause a denial of service (crash) or have other unspecified impact via crafted length values in an SSH_MSG_KEXINIT packet.
CVE-2016-0787	The diffie_hellman_sha256 function in kex.c in libssh2 before 1.7.0 improperly truncates secrets to 128 or 256 bits, which makes it easier for man-in-the-middle attackers to decrypt or intercept SSH sessions via unspecified vectors, aka a "bits/bytes confusion bug."
CVE-2019-13115	In libssh2 before 1.9.0, kex_method_diffie_hellman_group_exchange_sha256_key_exchange in kex.c has an integer overflow that could lead to an out-of-bounds read in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server. This is related to an _libssh2_check_length mistake, and is different from the various issues fixed in 1.8.1, such as CVE-2019-3855.
CVE-2019-17498	In libssh2 v1.9.0 and earlier versions, the SSH_MSG_DISCONNECT logic in packet.c has an integer overflow in a bounds check, enabling an attacker to specify an arbitrary (out-of-bounds) offset for a subsequent memory read. A crafted SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server.
CVE-2019-3855	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3856	An integer overflow flaw, which could lead to an out of bounds write, was discovered in libssh2 before 1.8.1 in the way keyboard prompt requests are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3857	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit signal are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3858	An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is received from the server. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-3859	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the _libssh2_packet_require and _libssh2_packet_requirev functions. A remote attacker who compromises a SSH server may be able to cause a Denial of

	Service or read data in the client memory.
CVE-2019-3860	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SFTP packets with empty payloads are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-3861	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH packets with a padding length value greater than the packet length are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-3862	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit status message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-3863	A flaw was found in libssh2 before 1.8.1. A server could send a multiple keyboard interactive response messages whose total length are greater than unsigned char max characters. This value is used as an index to copy memory causing in an out of bounds memory write error.
libtirpc 0.2.4-0.15.el7	
CVE-2018-14622	A null-pointer dereference vulnerability was found in libtirpc before version 0.3.3-rc3. The return value of makefd_xprt() was not checked in all instances, which could lead to a crash when the server exhausted the maximum number of available file descriptors. A remote attacker could cause an rpc-based application to crash by flooding it with new connections.
libxslt 1.1.28-5.el7	
CVE-2015-7995	The xsltStylePreCompute function in preproc.c in libxslt 1.1.28 does not check if the parent node is an element, which allows attackers to cause a denial of service via a crafted XML file, related to a "type confusion" issue.
CVE-2016-1683	numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles namespace nodes, which allows remote attackers to cause a denial of service (out-of-bounds heap memory access) or possibly have unspecified other impact via a crafted document.
CVE-2016-1684	numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles the i format token for xsl:number data, which allows remote attackers to cause a denial of service (integer overflow or resource consumption) or possibly have unspecified other impact via a crafted document.
logrotate 3.8.6-17.el7	
	None
lsof 4.87-6.el7	
	None
mailx 12.5-19.el7	
	None
nano 2.3.1-10.el7	
	None
nfs-utils 1.3.0-0.61.el7	
CVE-2019-3689	The nfs-utils package in SUSE Linux Enterprise Server 12 before and including version 1.3.0-34.18.1 and in SUSE Linux Enterprise Server 15 before and including version 2.1.1-6.10.2 the directory /var/lib/nfs is owned by statd:nogroup. This directory contains files owned and managed by root. If statd is compromised, it can therefore trick processes running with root privileges into creating/overwriting files anywhere on the system.
nodejs 8.16.0-1nodesource	
	None
nspr 4.19.0-1.el7_5	
	None

nss 3.36.0-7.1.el7_6	
CVE-2018-12384	When handling a SSLv2-compatible ClientHello request, the server doesn't generate a new random value but sends an all-zero value instead. This results in full malleability of the ClientHello for SSLv2 used for TLS 1.2 in all versions prior to NSS 3.39. This does not impact TLS 1.3.
CVE-2018-12404	A cached side channel attack during handshakes using RSA encryption could allow for the decryption of encrypted content. This is a variant of the Adaptive Chosen Ciphertext attack (AKA Bleichenbacher attack) and affects all NSS versions prior to NSS 3.41.
ntp 4.2.6p5-28.el7	
CVE-2015-7691	The crypto_xmit function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash) via crafted packets containing particular autokey operations. NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-9750.
CVE-2015-7692	The crypto_xmit function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash). NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-9750.
CVE-2015-7701	Memory leak in the CRYPTO_ASSOC function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (memory consumption).
CVE-2015-7702	The crypto_xmit function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash). NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-9750.
CVE-2015-7703	The "pidfile" or "driftfile" directives in NTP ntpd 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77, when ntpd is configured to allow remote configuration, allows remote attackers with an IP address that is allowed to send configuration requests, and with knowledge of the remote configuration password to write to arbitrary files via the :config command.
CVE-2015-7704	The ntpd client in NTP 4.x before 4.2.8p4 and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service via a number of crafted "KOD" messages.
CVE-2015-7705	The rate limiting feature in NTP 4.x before 4.2.8p4 and 4.3.x before 4.3.77 allows remote attackers to have unspecified impact via a large number of crafted requests.
CVE-2015-7849	Use-after-free vulnerability in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote authenticated users to possibly execute arbitrary code or cause a denial of service (crash) via crafted packets.
CVE-2015-7850	ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote authenticated users to cause a denial of service (infinite loop or crash) by pointing the key file at the log file.
CVE-2015-7852	ntpq in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash) via crafted mode 6 response packets.
CVE-2015-7853	The datalen parameter in the refclock driver in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to execute arbitrary code or cause a denial of service (crash) via a negative input value.
CVE-2015-7854	Buffer overflow in the password management functionality in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote authenticated users to cause a denial of service (daemon crash) or possibly execute arbitrary code via a crafted key file.
CVE-2015-7855	The decodenetnum function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (assertion failure) via a 6 or mode 7 packet containing a long data value.
CVE-2015-7871	Crypto-NAK packets in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to bypass authentication.

CVE-2015-7871	Crypto-NAK packets in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to bypass authentication.
CVE-2015-7974	NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 do not verify peer associations of symmetric keys when authenticating packets, which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key, aka a "skeleton key."
CVE-2016-4953	ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (ephemeral-association demobilization) by sending a spoofed crypto-NAK packet with incorrect authentication data at a certain time.
CVE-2016-4954	The process_packet function in ntp_proto.c in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (peer-variable modification) by sending spoofed packets from many source IP addresses in a certain scenario, as demonstrated by triggering an incorrect leap indication.
CVE-2016-4955	ntpd in NTP 4.x before 4.2.8p8, when autokey is enabled, allows remote attackers to cause a denial of service (peer-variable clearing and association outage) by sending (1) a spoofed crypto-NAK packet or (2) a packet with an incorrect MAC value at a certain time.
CVE-2016-4956	ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (interleaved-mode transition and time change) via a spoofed broadcast packet. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-1548.
CVE-2016-4957	ntpd in NTP before 4.2.8p8 allows remote attackers to cause a denial of service (daemon crash) via a crypto-NAK packet. NOTE: this vulnerability exists because of an incorrect fix for CVE-2016-1547.
CVE-2016-7426	NTP before 4.2.8p9 rate limits responses received from the configured sources when rate limiting for all associations is enabled, which allows remote attackers to cause a denial of service (prevent responses from the sources) by sending responses with a spoofed source address.
CVE-2016-7427	The broadcast mode replay prevention functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (reject broadcast mode packets) via a crafted broadcast mode packet.
CVE-2016-7428	ntpd in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (reject broadcast mode packets) via the poll interval in a broadcast packet.
CVE-2016-7429	NTP before 4.2.8p9 changes the peer structure to the interface it receives the response from a source, which allows remote attackers to cause a denial of service (prevent communication with a source) by sending a response for a source to an interface the source does not use.
CVE-2016-7431	NTP before 4.2.8p9 allows remote attackers to bypass the origin timestamp protection mechanism via an origin timestamp of zero. NOTE: this vulnerability exists because of a CVE-2-8138 regression.
CVE-2016-7433	NTP before 4.2.8p9 does not properly perform the initial sync calculations, which allows remote attackers to unspecified impact via unknown vectors, related to a "root distance that did not include the peer dispersion."
CVE-2016-7434	The read_mru_list function in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (crash) via a crafted mrulist query.
CVE-2016-9310	The control mode (mode 6) functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to set or unset traps via a crafted control mode packet.
CVE-2016-9311	ntpd in NTP before 4.2.8p9, when the trap service is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted packet.
CVE-2016-9312	ntpd in NTP before 4.2.8p9, when running on Windows, allows remote attackers to cause a denial of service via a large UDP packet.
CVE-2018-7170	ntpd in ntp 4.2.x before 4.2.8p7 and 4.3.x before 4.3.92 allows authenticated users that know the private symmetric key to create arbitrarily-many

	ephemeral associations in order to win the clock selection of ntpd and modify a victim's clock via a Sybil attack. This issue exists because of an incomplete fix for CVE-2016-1549.
CVE-2018-7184	ntpd in ntp 4.2.8p4 before 4.2.8p11 drops bad packets before updating the "received" timestamp, which allows remote attackers to cause a denial of service (disruption) by sending a packet with a zero-origin timestamp causing the association to reset and setting the contents of the packet as the most recent timestamp. This issue is a result of an incomplete fix for CVE-2-7704.
CVE-2018-7185	The protocol engine in ntp 4.2.6 before 4.2.8p11 allows a remote attackers to cause a denial of service (disruption) by continually sending a packet with a zero-origin timestamp and source IP address of the "other side" of an interleaved association causing the victim ntpd to reset its association.
openldap 2.4.44-21.el7_6	
CVE-2017-14159	slapd in OpenLDAP 2.4.45 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill \`cat /pathname\`" command, as demonstrated by openldap-initscript.
CVE-2017-17740	contrib/slapd-modules/nops/nops.c in OpenLDAP through 2.4.45, when both the nops module and the memberof overlay are enabled, attempts to free a buffer that was allocated on the stack, which allows remote attackers to cause a denial of service (slapd crash) via a member MODDN operation.
CVE-2017-9287	servers/slapd/back-mdb/search.c in OpenLDAP through 2.4.44 is prone to a double free vulnerability. A user with access to search the directory can crash slapd by issuing a search including the Paged Results control with a page size of 0.
CVE-2019-13057	An issue was discovered in the server in OpenLDAP before 2.4.48. When the server administrator delegates rootDN (database admin) privileges for certain databases but wants to maintain isolation (e.g., for multi-tenant deployments), slapd does not properly stop a rootDN from requesting authorization as an identity from another database during a SASL bind or with a proxyAuthz (RFC 4370) control. (It is not a common configuration to deploy a system where the server administrator and a DB administrator enjoy different levels of trust.)
CVE-2019-13565	An issue was discovered in OpenLDAP 2.x before 2.4.48. When using SASL authentication and session encryption, and relying on the SASL security layers in slapd access controls, it is possible to obtain access that would otherwise be denied via a simple bind for any identity covered in those ACLs. After the first SASL bind is completed, the sasl_ssf value is retained for all new non-SASL connections. Depending on the ACL configuration, this can affect different types of operations (searches, modifications, etc.). In other words, a successful authorization step completed by one user affects the authorization requirement for a different user.
policycoreutils 2.5-29.el7_6.1	
	None
polkit 0.112-18.el7_6.1	
CVE-2018-1116	A flaw was found in polkit before version 0.116. The implementation of the polkit_backend_interactive_authority_check_authorization function in polkitd allows to test for authentication and trigger authentication of unrelated processes owned by other users. This may result in a local DoS and information disclosure.
procps-ng 3.3.10-23.el7	
CVE-2018-1122	procps-ng before version 3.3.15 is vulnerable to a local privilege escalation in top. If a user runs top with HOME unset in an attacker-controlled directory, the attacker could achieve privilege escalation by exploiting one of several vulnerabilities in the config_file() function.

CVE-2018-1123	procps-ng before version 3.3.15 is vulnerable to a denial of service in ps via mmap buffer overflow. Inbuilt protection in ps maps a guard page at the end of the overflowed buffer, ensuring that the impact of this flaw is limited to a crash (temporary denial of service).
CVE-2018-1124	procps-ng before version 3.3.15 is vulnerable to multiple integer overflows leading to a heap corruption in file2strvec function. This allows a privilege escalation for a local attacker who can create entries in procfs by starting processes, which could result in crashes or arbitrary code execution in proc utilities run by other users.
CVE-2018-1125	procps-ng before version 3.3.15 is vulnerable to a stack buffer overflow in pgrep. This vulnerability is mitigated by FORTIFY, as it involves strncat() to a stack-allocated string. When pgrep is compiled with FORTIFY (as on Red Hat Enterprise Linux and Fedora), the impact is limited to a crash.
CVE-2018-1126	procps-ng before version 3.3.15 is vulnerable to an incorrect integer size in proc/alloc.* leading to truncation/integer overflow issues. This flaw is related to CVE-2018-1124.
quota 4.01-17.el7	
	None
rpm 4.11.3-35.el7	
CVE-2013-6435	Race condition in RPM 4.11.1 and earlier allows remote attackers to execute arbitrary code via a crafted RPM file whose installation extracts the contents to temporary files before validating the signature, as demonstrated by installing a file in the /etc/cron.d directory.
CVE-2017-7501	It was found that versions of rpm before 4.13.0.2 use temporary files with predictable names when installing an RPM. An attacker with ability to write in a directory where files will be installed could create symbolic links to an arbitrary location and modify content, and possibly permissions to arbitrary files, which could be used for denial of service or possibly privilege escalation.
rsync 3.1.2-4.el7	
CVE-2017-15994	rsync 3.1.3-development before 2017-10-24 mishandles archaic checksums, which makes it easier for remote attackers to bypass intended access restrictions. NOTE: the rsync development branch has significant use beyond the rsync developers, e.g., the code has been copied for use in various GitHub projects.
CVE-2017-16548	The receive_xattr function in xattrs.c in rsync 3.1.2 and 3.1.3-development does not check for a trailing '\0' character in an xattr name, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact by sending crafted data to the daemon.
CVE-2017-17433	The recv_files function in receiver.c in the daemon in rsync 3.1.2, and 3.1.3-development before 2017-12-03, proceeds with certain file metadata updates before checking for a filename in the daemon_filter_list data structure, which allows remote attackers to bypass intended access restrictions.
CVE-2017-17434	The daemon in rsync 3.1.2, and 3.1.3-development before 2017-12-03, does not check for fnamecmp filenames in the daemon_filter_list data structure (in the recv_files function in receiver.c) and also does not apply the sanitize_paths protection mechanism to pathnames found in "xname follows" strings (in the read_ndx_and_attrs function in rsync.c), which allows remote attackers to bypass intended access restrictions.
CVE-2018-5764	The parse_arguments function in options.c in rsyncd in rsync before 3.1.3 does not prevent multiple --protect-args uses, which allows remote attackers to bypass an argument-sanitization protection mechanism.
rsyslog 8.24.0-34.el7	
CVE-2017-12588	The zmq3 input and output modules in rsyslog before 8.28.0 interpreted description fields as format strings, possibly allowing a format string attack with

	unspecified impact.
CVE-2018-16881	A denial of service vulnerability was found in rsyslog in the imptcp module. An attacker could send a specially crafted message to the imptcp socket, which would cause rsyslog to crash. Versions before 8.27.0 are vulnerable.
sudo 1.8.23-3.el7	
CVE-2019-14287	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#$((0xffffffff))" command.
CVE-2019-18684	** Sudo through 1.8.29 allows local users to escalate to root if they have write access to file descriptor 3 of the sudo process. This occurs because of a race condition between determining a uid, and the setresuid and openat system calls. The attacker can write "ALL ALL=(ALL) NOPASSWD:ALL" to /proc/#####/fd/3 at a time when Sudo is prompting for a password. NOTE: This has been disputed due to the way Linux /proc works. It has been argued that writing to /proc/#####/fd/3 would only be viable if you had permission to write to /etc/sudoers. Even with write permission to /proc/#####/fd/3, it would not help you write to /etc/sudoers.
systemd 219-62.el7_6.9	
CVE-2017-1000082	systemd v233 and earlier fails to safely parse usernames starting with a numeric digit (e.g. "0day"), running the service in question with root privileges rather than the user intended.
CVE-2017-18078	systemd-tmpfiles in systemd before 237 attempts to support ownership/permission changes on hardlinked files even if the fs.protected_hardlinks sysctl is turned off, which allows local users to bypass intended access restrictions via vectors involving a hard link to a file for which the user lacks write access, as demonstrated by changing the ownership of the /etc/passwd file.
CVE-2018-1049	In systemd prior to 234 a race condition exists between .mount and .automount units such that automount requests from kernel may not be serviced by systemd resulting in kernel holding the mountpoint and any processes that try to use said mount will hang. A race condition like this may lead to denial of service, until mount points are unmounted.
CVE-2018-15686	A vulnerability in unit_deserialize of systemd allows an attacker to supply arbitrary state across systemd re-execution via NotifyAccess. This can be used to improperly influence systemd execution and possibly lead to root privilege escalation. Affected releases are systemd versions up to and including 239.
CVE-2018-15687	A race condition in chown_one() of systemd allows an attacker to cause systemd to set arbitrary permissions on arbitrary files. Affected releases are systemd versions up to and including 239.
CVE-2018-15688	A buffer overflow vulnerability in the dhcp6 client of systemd allows a malicious dhcp6 server to overwrite heap memory in systemd-networkd. Affected releases are systemd: versions up to and including 239.
CVE-2018-16864	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when a program with long command line arguments calls syslog. A local attacker may use this flaw to crash systemd-journald or escalate his privileges. Versions through v240 are vulnerable.
CVE-2018-16865	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when many entries are sent to the journal socket. A local attacker, or a remote one if systemd-journal-remote is used, may use this flaw to crash systemd-journald or execute code with journald privileges. Versions through v240 are vulnerable.

CVE-2018-16888	It was discovered systemd does not correctly check the content of PIDFile files before using it to kill processes. When a service is run from an unprivileged user (e.g. User field set in the service file), a local attacker who is able to write to the PIDFile of the mentioned service may use this flaw to trick systemd into killing other services and/or privileged processes. Versions before v237 are vulnerable.
CVE-2018-6954	systemd-tmpfiles in systemd through 237 mishandles symlinks present in non-terminal path components, which allows local users to obtain ownership of arbitrary files via vectors involving creation of a directory and a file under that directory, and later replacing that directory with a symlink. This occurs even if the fs.protected_symlinks sysctl is turned on.
CVE-2019-3844	It was discovered that a systemd service that uses DynamicUser property can get new privileges through the execution of SUID binaries, which would allow to create binaries owned by the service transient group with the setgid bit set. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the GID will be recycled.
tar 1.26-35.el7	
CVE-2019-9923	pax_decode_header in sparse.c in GNU Tar before 1.32 had a NULL pointer dereference when parsing certain archives that have malformed extended headers.
util-linux 2.23.2-59.el7_6.1	
CVE-2017-2616	A race condition was found in util-linux before 2.32.1 in the way su handled the management of child processes. A local authenticated attacker could use this flaw to kill other processes with root privileges under specific conditions.
yum 3.4.3-161.el7	
CVE-2014-0022	The installUpdates function in yum-cron/yum-cron.py in yum 3.4.3 and earlier does not properly check the return value of the sigCheckPkg function, which allows remote attackers to bypass the RMP package signing restriction via an unsigned package.
zip 3.0-11.el7	
CVE-2018-13410	** Info-ZIP Zip 3.0, when the -T and -TT command-line options are used, allows attackers to cause a denial of service (invalid free and application crash) or possibly have unspecified other impact because of an off-by-one error. NOTE: it is unclear whether there are realistic scenarios in which an untrusted party controls the -TT value, given that the entire purpose of -TT is execution of arbitrary commands.
zlib 1.2.7-18.el7	
	None

Table 7: Potential Vulnerabilities Identified

5.2 Static Code Analysis & Documentation Review

Table 8: Summary of Issues Discovered During the Static Code summarizes the findings that arose from the source code review team's assessment of the voting system. Potential exploitation of a weakness or vulnerability and type of attacker is noted where applicable.

#	Description	Assessment	Developer Response	Severity
1	The cryptographic code is not running in a FIPS 140-2 approved environment. The cryptohelper code makes use of OpenSSL code and documentation refers to FIPS 140-2 certificate 2747. The README.md file states that openSSL or openSSL 1.1 can be installed The certificate is only for the FIPS container package and that is only for OpenSSL 1.0.x. The CentOS which is used is not listed on certificate. The authentication code makes use of cryptohelper code from a public source. The code attempts to setup in FIPS mode. The cryptohelper code calls OpenSSL code that is installed on the system. According to README.md file the admin can install OpenSSL (1.0.x) or OpenSSL 1.1. There is a file under cryptohelper folder doc.go that mentions FIPS 140-2 certificate 1747, which is for OpenSSL Crypto Container, and that is based on OpenSSL 1.0.x. If the voting system requires the code running to be FIPS 140-2 approved, it needs to be running in an approved environment and needs to ensure the level of OpenSSL stated in the certificate is installed.	Non-compliance with voting system requirements. The CVSS section 2.4.4.1 requires a FIPS 140-2 validated module. The doc.go file and other documentation states that CentOS 7.6.1810 is the Operating System in use. This is not one of the Operating Environments listed in CMVP certificate 1747 for the OpenSSL module.	"The Tally and VBL systems use open SSL as packaged and distributed by CentOS. The Cryptohelper library (written by the same team as Tally) abstracts the use of OpenSSL to make it safer to work with and ensure it is always put in FIPS mode. The version of OpenSSL being used is "openssl-1.0.2k-16.el7_6.1.x86_64.rpm" as found in the installer repo at "rpms/yums/x86_64/7/updates/packages/openssl-1.0.2k-16.el7_6.1.x86_64.rpm" Tally and VBL use the Red Hat FIPS verified OpenSSL package (openssl-1.0.2k-16.el7_6.1.x86_64.rpm as distributed by CentOS. CVSS only requires that the module is verified and not that the cryptographic module is running on a FIPS verified hardware configuration."	Low
2	The code does not use structured exception handling as specified in CVSS. The errors within functions are logged and an	Non-compliance with voting system standards. In section 5.2.2 of the	"The "PriorityErrorHandeler" as outlined in this report is outside of the shared library (bitbucket.org/vsap/common/*) and is in the	Non (reduced from Low

#	Description	Assessment	Developer Response	Severity
	event is passed to an error handler which looks like could be in host application (outside of code base we have in hand)	CVSS document it states that the programming language should use structured exception handling. The code returns an error condition that is checked for nil value and if not nil will log an event with the error condition and set an event to be handled. The code to handle the error event could be outside the code being reviewed.	implementing service libraries. This puts it outside of the shared library we developed to allow us to reuse code, but inside the Tally/VBL code bases. This call provides an optional registration where an implementing service can be notified of major errors to allow them to be reported centrally to a system user using context that the shared library doesn't have. In the auth service, this registration was not found because the auth service does not make use of this feature. This is exactly why routeToPriorityErrorHandler starts with a nil check on the function. This registration can, however, be found in most of the services inside tally-core. For example, the tallymanager service registers it here: cmd/production/tallymanager/main.go . Whether or not a given service opts in to this callback, that is compiled into the deployed executable so nothing on the system can later decide to register this callback once the executable is compiled."	due to response)
3	The code has some hardcoded passwords. A person with access to code could learn or change the passwords. The code makes use of DB_PASS, MYSQL_ROOT_PASS, KAFKA_PASS, SQL_PASS and some yml, yaml, cql and sql files.	Possible unauthorized access or loss of access due to a changed password. The hardcoded passwords can be read by someone with access to the code and that person could get access when it should be unauthorized. They could also change the password to prevent others from gaining access.	"The report outlines a variety of apparent hard coded passwords. We have reviewed the relevant files and want to clarify each case." See Table 9: Response to Finding 3, Hard Coded Passwords in Appendix A: Response to Finding 3, Hard Coded Passwords for details of the response to each instance.	Non (reduced from Medium due to response)
4	SHA-512 sum of file is incorrect and likely	The code could have been	"It is unclear to us where the file	Non

#	Description	Assessment	Developer Response	Severity
	manually edited. In TDA1 package folder, there are two files: vba_deployment.tgz and vba_deployment.tgz.sha512. Running a sha512sum on the file vba_deployment.tgz shows the same string, except for one character. This indicates one of two possibilities: ● The hash value in the .sha512 file was manually edited. ● We've discovered a one-char deviated hash collision, which is extremely unlikely in particular of the contents of the .tgz file was modified. If it was, then the hash value would be entirely different, rather than one character difference as found on test.	replaced or the sha512sum was replaced. It is unclear to the tester whether the file vba_deployment.tgz is therefore the correct file.	"vbl_deployment.tgz.sha512" came from. Our deployment package did not generate that file. Moreover, "sha512sum vbl_deployment.tgz" for us generates the hash: SHA512(/tmp/vbl_deployment.tgz)= 0cee9e3b3e0058d8f7ee6dafc0ea3116e9877e3e58c156c83a8f8d51d2415659913a80dc05da164a70e6432eae72d223f 617ccafea44eefc845d3bc1564b0e70 This matches the hash reported by the build system when the trusted build was made. These flash drives were not originally planned as a primary means of delivery of code/builds to you. As such, they may have had previous VBL builds. particularly if there is another VBL_deployment.tgz set on one of the flash drives, it is possible that these files are a previous build. If you can tell us where your hashes come from, we may be able to shed more light on this.	(reduced from Low due to response)
5	The CVSS documents call for cryptographic functions from a FIPS module in several places and some items appear to not meet that requirement. The CVSS document in section 2.4.4.2 mentions a DRBG should be used to randomize the ballot image order. No evidence could be found that shows the ballot image would be randomized, although the code did have a random function. In section 7.6.1 of the CVSS it states to use a MAC to verify receipt of the ballot, no evidence was found that the ballot is verified using a MAC. In section 9.6.7 it mentions to list all crypto used, provide the FIPS module name, map all	Non-compliance with voting system requirements. The crypto code documented in VSAP-TDP-005_ System_ Security_ Specification section 9.3 is in historical status for using AES and Triple-DES key wrapping, the OpenSSL module is not documented. Not all of the cryptographic requirements defined in the CVSS document appear to be met.	In reference to section 2.4.4.2 of the CVSS: "This is only a CVSS requirement when tabulating DRE generated ballot images. Note that the requirement for the DRE recording ballots in a randomized order is outlined in section 7.7.3 and note that all of 7.7 is specific to DREs. This section contains requirements for DREs with a Voter Verifiable Paper Audit Trail (VVPAT) component... Due to VSAP being a paper based system Tally is not subject to this requirement." In reference to section 7.6.1 of the CVSS: "CVSS requires detection of transmission errors and, when encryption is used, it must be NIST approved and at least 112 bits ("This should	Low

#	Description	Assessment	Developer Response	Severity
	crypto functions to voting system functions, and describe key creation, storage, etc. While the VSAP-TDP-005 document did have some of this in sections 9.1 – 9.4 it did not have information on the OpenSSL functions used, or how they map to the voting system. The OpenSSL module name was defined in a doc.go file as well as the certificate, it is not mentioned in the VSAP-TDP-005 document.		include standard transmission error detection and correction methods such as checksums or message digest hashes”). All messages passed over the network are transmitted over TCP/IP which provides built in integrity checks. Additionally, much of the data transferred is over TLS with its own checksums. All images are further signed on disk when ingested into Tally. Nothing in this section requires encryption or MAC usage in any particular part of the system, just that the cryptography must be strong when used.” In reference to section 9.6.7 of the CVSS: “We are working with Smartmatic to provide an updated TDP that aims to clarify and document these questions better. Please let us know if that does not adequately address these questions.”	
6	The BMG code has calls to encode passwords and for signature verification that do not appear to be FIPS 140-2 certified. The WebSecurityConfiguration.java file has calls to BcryptPasswordEncoder to hash passwords. The Bcrypt library used is not FIPS 140-2 certified. The BmgConfiguration.java and CertificateUtilService.java make calls to java.security.Signature, since the type of Java used is not known it might not be FIPS 140-2 certified.	Non-compliance with voting system requirements. The CVSS section 2.4.4.1 requires FIPS 140-2 validated module. The use of BcryptPasswordEncoder and java.security.X509Certificate functions do not appear to be FIPS 140-2 certified. The crypto code is not running in a a FIPS 140-2 approved environment.	“These findings relate to the CMVP listings at NIST for this combination of hardware and software. A discussion with the State is requested.”	Low
7	The BMD code has calls to encode passwords that do not appear to be FIPS 140-2 certified. The BMD code has calls to bcrypt.hash and	Non-compliance with voting system requirements.	“These findings relate to the CMVP listings at NIST for this combination of hardware and software. A discussion with the State is	Low

#	Description	Assessment	Developer Response	Severity
	other functions within the bcrypt library.	The CVSS section 2.4.4.1 requires FIPS 140-2 validated module. The use of Bcrypt functions do not appear to be FIPS 140-2 certified. The crypto code is not running in a a FIPS 140-2 approved environment.	requested.”	
8	The CVSS states in section 9.6.7 that cryptographic information needs to be documented. In the VSAP-TDP-005_System_Security_Specification.pdf document it only mentions use of the HSM module and states the CMVP certificate for that module. In reviewing the code, it was found that the bcrypt module is used for hashing passwords. A call to the genSalt function was also found. Use of bcrypt is not documented. In the code review it was also found that the Java security function signature.verify was used. The Java security runtime environment is also not documented.	Non-compliance with voting system standards. Requirements for section 5.2.8 in CVSS document appear to not be met.	“The technical documentation was updated 17 September. Please review and let us know if there are additional concerns.”	Non (reduced from low due to response)
9	CVSS section 5.2.5(a) calls for proper exception handling to be done by the application. A search of the code in BMD shows that exception handling is being done. The BMD code has calls to try/catch/finally in order to handle exceptions. A search of the BMG Java and JavaScript code shows proper exception handling as well.	Requirements for section 5.2.5(a) in CVSS document appear to be met.	No response required. (non-finding)	Non
10	CVSS section 5.2.8 calls for input range checking to be done by the application. A search of the code in both BMD and BMG	Requirements for section 5.2.8 in CVSS document appear to be met.	No response required. (non-finding)	Non

#	Description	Assessment	Developer Response	Severity
	show that range checking is being done. The BMD code had checks and then would log rangeError msgs. Also in the BMG code the UI input values were checked and would return an invalid flag/state if the check was bad.			
11	Audit log files are stored in the BMD device. Audit and usage logs get sent to BMG. The audit log is named BEL.log (BMD Election Logs). The BMD implements automatic audit events through the auditLogEvent function which sends and event to be logged in the system files. Examples include the functions which invoke the auditLogEvent Function such as componentDidMount() and mouseUp().	Auditing is implemented well using the auditLogEvent function.	No response required. (non-finding)	Non
12	No default values are set for lockout policies or invalid password attempts. The JavaScript that implements lockout rules doesn't set any defaults; It's left to the admin and governmental policy to decide what's appropriate. The CVSS section 7.2.3 requires that the voting system enforce temporary lockout min/max, permanent lockout min/max, lockout interval, and finally invalid attempts min/max. The voting system does enforce whatever is set by the admin, but the admin could in theory decide not to set minimum values for these variables. Thus, while it's ideal that the admin would take these into consideration, or the governmental body that sets them up may have minimum values in mind it's not a guarantee. The potential for abuse is therefore present regardless of likelihood.	No default values for lockout, invalid attempts or timeout could be exploited by a malicious actor. Adheres to Section 7.2.3 of voting system standard, but does not set default minimums.	"The admin shall be able to decide the lockout configuration to comply with CVSS requirement 7.2.3 f: *'7.2.3 f. f. Voting systems **shall** allow the administrator group or role to configure the account lock out policy, including the time period within which failed attempts must occur, the number of consecutive failed access attempts allowed before lock out, and the length of time the account is locked out.'* Additionally, the minimum values are set to values different from 0..." Therefore, BMG system ensures that even an Admin cannot set values less than those minimal values.	Non (reduced from Low due to response)
13	No minimum values set for password length,	Non-compliance with	"The admin shall be able to decide about the	Non

#	Description	Assessment	Developer Response	Severity
	complexity, or history count. The JavaScript that implements password changes and history does not take into consideration complexity of the password, or minimum length. The CVSS section 7.2.3 requires that the voting system enforce password strength, history, and expiration. The voting system does enforce whatever is set by the admin, but the admin could in theory decide not to set minimum values for these variables. Thus, while it's ideal that the admin would take these into consideration, or the governmental body that sets them up may have minimum values in mind it's not a guarantee. The potential for abuse is therefore present regardless of likelihood.	voting system requirements section 7.2.3 g-k. No minimum values set within the code leaves an attack surface open to potential identity theft.	enforcement of password strength, histories, and expiration to comply with CVSS requirement 7.2.3 g: *'7.2.3 g. If the voting system uses a user name and password authentication method, the voting system shall allow the administrator to enforce password strength, histories, and expiration.'* Additionally, the minimum values that an Admin can set are different from 0, as is shown in the picture below: And the maximum values accepted by the system are as is shown in the next picture: Therefore, BMG system ensures that even an Admin cannot set values less/more than those minimum/maximum values."	(reduced from Low due to response)
14	The package files and a README file show conflicting version of bcrypt being used.	Could cause unreliable results when calling the different versions of library functions.	"We are not calling the bcrypt function, so this discrepancy has no effect on BMD function."	Non (reduced from Medium due to response)
15	Third-party code provides an attack vector and must be monitored for changes and reviewed when they occur. Third-party code is included which allows other coders to contribute functionality into the system. While efficient for the sake of functionality, this creates significant attack potential. Unfortunately, this potential cannot be quantified since it depends on the specific use of the third-party code in question and what functionality might be inserted. 182 package.json files exist in the source code reviewed, the vast majority in the BMD code	Use of third-party code is not in and of itself a finding, but great care must be taken to ensure malicious functionality is not introduced into code not under local control. All changes should be reviewed, no code should be included in the system automatically. The volume of third-party code and the variety of sources from which it is obtained is the	All third party code is reviewed before implementation into the system. Will continue to monitor potential threats/risks with third party software. Can provide review results of third party code.	Low (reduced from Medium due to response)

#	Description	Assessment	Developer Response	Severity
	tree. These files contain information about many third-party JavaScript tools pulled from npmjs.com, github.com, and other repositories of third-party open-source tools. Third-party code is not under control of the product developer, therefore it is their responsibility to monitor and verify the content. The developer must also monitor publicly known vulnerabilities to be aware of flaws and fixes so they can be addressed in a timely manner. The majority of third-party code referenced is maintained on github.com. This means anyone with access to those repositories can make an update to that code. A malicious contributor could conceivably update the code on GitHub knowing it will later be imported into an update of the voting system. Some of the references in package.json files include SHA-1 hash values which should prevent a malicious download from being accepted (assuming this value is verified by the installation software). However, this is not always the case. Some code appears to be imported from a local IP address, thus those copies are assumed to be static and updated manually using known content and should not pose as high a risk.	finding because of the increased possibility for attack. Risk may be considered acceptable provided all new code is reviewed and all imported code is verified at the time of import. Any automatic import of code from a third-party repository (e.g., GitHub) without confirmation that the content is as expected would allow for malicious injection of functionality.		
16	SQL database initialization seed data is entirely optional, and INSERT IGNORE can lead to unforeseen consequences. The initial comment in the SQL table data import reads “This will insert static data **needed** for BMG”. This indicates, or at least	The initial state of the BMG could be unrecoverable or badly formed data could be imported because no errors are generated.	The word 'needed' in this context should be taken as 'used'. Moreover, this script is used only once during deployment, and the results obtained during the tests performed are successful.	Low

#	Description	Assessment	Developer Response	Severity
	implies that the contents of the .sql file are required. Therefore INSERT IGNORE is inappropriate, and should probably be removed. Another hidden feature of this syntax is that erroneous data can be imported into the database in the wrong fields, because MySQL will simply massage that data to fit the field type automatically. For example, a DATETIME data piece could be converted into an INT on import, because INSERT IGNORE was present.	MySQL will instead of failing on a bad insert, simply **convert** the data into a format that fits. In other words: INSERT IGNORE can lead to incorrect data imported into the database. Bugs generated from it could be potentially missed, and therefore abused by a malicious attacker. See data should be properly formatted to avoid insertion failures, therefore the use of INSERT IGNORE is inappropriate.		
17	Database creation sets only_full_group_by to null, creating the possibility of inconsistent data on select. In the BMG database table generation script, one line is problematic: SET GLOBAL sql_mode=(SELECT REPLACE(@@sql_mode,'ONLY_FULL_GROUP_BY','')); Versions prior to MySQL 5.7.5 would make sense to adjust/remove the group by restriction, because it was considered "too strict" by most. In particular it would enforce the use of the group by clause inappropriately in situations where it was simply not necessary. Versions of MySQL after 5.7.5 take into consideration the relative deterministic values returned from queries properly, and is far less of an issue than before this version. In effect, the issues associated with	MySQL allows for adjusting sql_mode, such that group by restrictions aren't maintained, which could lead to "random" results being obtained from incorrect queries. This vulnerability applies to versions of MySQL prior to 5.7.5. sql_mode should not be altered, so that non-deterministic queries, and therefore unpredictable values, are not returned to BMG.	The results obtained with the current BMG version code against these settings are successful. Removing this setting may cause issues.	Low

#	Description	Assessment	Developer Response	Severity
	ONLY_FULL_GROUP_BY have been fixed. Hence, this line is not recommended as it could lead to erroneous SQL queries that would return incorrect values, or at the very least unpredictable values due to non-deterministic queries.			
18	Static code analysis of Go source code. A scan of Go source code was performed using the GoLang Lint tool found at https://github.com/golang/lint. This produced numerous informational and warning messages. A very large number of comments concerned malformed comments around exported names or that they should be unexported. These and others may be overly cautious warnings about syntax, including things like: • 428 warnings of if/then/else construction • 204 complaints about use of += 1 and -= 1 instead of ++ and -- • 85 warnings about range specification • However, other messages indicate a problem that could cause unintended behavior: • 12 warnings of blank imports • 97 warnings of returns unexported	The higher potential warnings are included in an accompanying text file to this finding (i.e. same name but with a .txt extension). These should be reviewed by the development team to determine whether they could represent any issue.	"The number of errors that are being reported are partially due to the repos being copied over several times. Based on the feedback there appears to be: • 3 copies of the Tally source code (2 old and 1 current) • 4 copies of the Auth source code (2 old and 2 current) • 5 copies of the Logviewer source code (3 old and 2 current) • 3 copies of the Ballot Layout source code (2 old and 1 current) This increases the apparent number of errors, since the majority of the issues identified are duplicated across each copy of the repo. With regards to the issues called out, all paths reviewed were inside /vendor. In Go, the vendor path is used for external dependencies (e.g. third party libraries) that were not authored by the Tally/VBL/VSAP teams. All items listed below are stock third party and occur in at least one of the following repositories: **Tally** • OLD/TDA3.local/OLD/tally-core/tally-core/vendor (appears to not be latest code) • OLD/TDA3.local/tally-core/tally-core/vendor/ (appears to not be latest code) • TallySource/tally-core/vendor/	Low (reduced from Medium due to response)

#	Description	Assessment	Developer Response	Severity
			Auth • OLD/TDA3.local/auth-service/auth-service/vendor (appears to not be latest code) • OLD/TDA3.local/OLD/auth-service/auth-service/vendor (appears to not be latest code) • TallySource/auth-service/vendor/ • VBL_source_and_Keys/auth-service/vendor/Log viewer • OLD/TDA1.local/logviewer-service/logviewer-service/vendor (appears to not be latest code) • OLD/TDA3.local/logviewer-service/logviewer-service/vendor (appears to not be latest code) • OLD/TDA3.local/OLD/logviewer-service/logviewer-service/vendor (appears to not be latest code) • TallySource/logviewer-service/vendor/ • VBL_source_and_Keys/logviewer-service/vendor/ **Ballot Layout** • OLD/TDA1.local/ballot-layout/ballot-layout/vendor/ • OLD/TDA1.local/ballot-layout/vendor/ • VBL_source_and_Keys/ballot-layout/vendor/ These entries are: **Warning: “exported method (or func) * returns unexported type *, which can be annoying to use”:** These items are test code: Shopify/sarama/mockresponses.go:29:59: Shopify/sarama/mockresponses.go:61:60: Shopify/sarama/mockresponses.go:105:64: Shopify/sarama/mockresponses.go:164:62: Shopify/sarama/mockresponses.go:240:61:	

#	Description	Assessment	Developer Response	Severity
			Shopify/sarama/mockresponses.go:324:71: Shopify/sarama/mockresponses.go:373:70: Shopify/sarama/mockresponses.go:420:67: Shopify/sarama/mockresponses.go:477:62: Shopify/sarama/mockresponses.go:530:66: Shopify/sarama/mockresponses.go:550:67: Shopify/sarama/mockresponses.go:569:67: Shopify/sarama/mockresponses.go:588:71: Shopify/sarama/mockresponses.go:607:68: Shopify/sarama/mockresponses.go:630:70: Shopify/sarama/mockresponses.go:656:67: Shopify/sarama/mockresponses.go:677:65: Shopify/sarama/mockresponses.go:695:63: Shopify/sarama/mockresponses.go:717:65: stretchr/testify/mock/mock.go:620:32 testify/mock/mock.go:532:32 Production code written to allow for testing: gocql/gocql/host_source.go:286:30: gocql/gocql/host_source.go:299:28 hashicorp/go-sockaddr/ifaddrs.go:46:49 hashicorp/go-sockaddr/route_info_bsd.go:17:22 hashicorp/go-sockaddr/sockaddrs.go:32:45 modern-go/reflect2/reflect2.go:136:27 k8s.io/apimachinery/pkg/util/strategicpatch/types.go:48:50 k8s.io/apimachinery/pkg/util/strategicpatch/types.go:111:51 Although the linter is correct that this can be annoying, this is done intentionally in test code where a mock object is returned that implements the same interface as the real object to allow for better control and injection of test harnesses into unit test code. In production code this pattern allows unit tests to simulate the state the code under test is running in	

#	Description	Assessment	Developer Response	Severity
			to better check code behavior. **Warning: "a blank import should only be in a main or test package, or have a comment justifying it":** This error only occurs in support packages officially published by the Go team (although it occurs in several copies of the tally-core repo that were scanned: golang.org/x/crypto/openpgp/read.go:10:2 golang.org/x/crypto/openpgp/packet/public_key.go:15:2 golang.org/x/crypto/ssh/common.go:15:2 The same warning**: "a blank import should be only in a main or test package, or have a comment justifying it"** does occur once in a library that the ballot layout team has modified. This code ("bitbucket.org/vsap/pdf/image_obj.go:7:2") occurs three times in the scan results as the results seem to include three coppies of the VBL repo. Although this is a library that we had to modify, this file remains unchanged. When updating the library, it was deemed safer to leave imports that we were not impacting alone rather than trying to change things that could have been done stylistically better."	
19	Static code analysis of JavaScript source code. A scan of JavaScript code was performed using the JavaScript Lint tool found at javascriptlint.com. This produced numerous informational and warning messages. Many may be overly cautious warnings about syntax, including things like: • 1973 warnings block statements containing block statements should use	The higher potential warnings are included in an accompanying text file to this finding (i.e. same name but with a .txt extension). These should be reviewed by the development team to determine whether they	"In this item, like 18, it appears that several repositories are mixed together. We are ignoring the "OLD/BMD_Code/", as that is not our area to respond. We are also ignoring: • OLD/TDA1.local/ballot-layout/* • OLD/TDA1.local/logviewer-service/* • OLD/TDA1.local/vbl_deployment/* • OLD/TDA3.local/OLD/auth-service/* • OLD/TDA3.local/OLD/logviewer-service/*	Low (reduced from Medium due to response)

#	Description	Assessment	Developer Response	Severity
	curly braces to resolve ambiguity • 1464 warnings that comparisons against null, 0, true, false, or an empty string allow implicit type conversion so === or !== should be used • 858 warnings that functions do not always return a value • 118 warnings of variable redeclarations • 20 warnings where using parseInt is missing a radix parameter (but default behavior is defined) • 12 warnings about missing default case statements in a switch statement However, other messages indicate a problem that could cause unintended behavior: • 207 warnings that an else statement could be matched with one of multiple if statements • 48 warnings of useless comparisons using identical expressions • 21 warnings of unknown order of operations for successive plus or minus signs (x+++y or x---y)	could represent any issue.	• OLD/TDA3.local/OLD/tally-core/* • OLD/TDA3.local/auth-service/* • OLD/TDA3.local/logviewer-service/* • OLD/TDA3.local/tally-core/* These paths/repos seem to have been superseded by: • TallySource/auth-service/* • TallySource/logviewer-service/logviewer/* • TallySource/tally-core/* • VBL_source_and_Keys/auth-service/* • VBL_source_and_Keys/ballot-layout/* • VBL_source_and_Keys/logviewer-service/* Even here there is a significant amount of duplication, but it brings the total number of findings down to 91. Further review shows that these are actually only 13 distinct issues. Twelve are in Jquery in the file “jquery-3.2.1.min.js” • 2:lint warning: useless comparison; comparing identical expressions • 2:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) • 2:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) • 3:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) • 3:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) • 3:lint warning: the else statement could be	

#	Description	Assessment	Developer Response	Severity
			matched with one of multiple if statements (use curly braces to indicate intent) ● 3:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 3:lint warning: useless comparison; comparing identical expressions ● 4:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 4:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 4:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) ● 4:lint warning: unknown order of operations for successive plus (e.g. x+++y) or minus (e.g. x---y) signs Jquery is a major project. While we have not analyzed these findings code use cases, there seem to be no CVEs related to them. Additionally, this is checking *minified* code - meaning that it has been post processed to make it as small as possible. It appears that most of these warnings are stylistic to avoid confusion, as such, while valid in code that would be read by humans, are likely not relevant to minified source code as the computer will not treat them as ambiguous or unclear. There was also one identified issue in bootstrap-table.min.js (although it was identified multiple times) that appears to be the same case as the JQuery issues.	

#	Description	Assessment	Developer Response	Severity
			bootstrap-table.min.js:7:lint warning: the else statement could be matched with one of multiple if statements (use curly braces to indicate intent) Like the JQuery issues above, this is likely due to scanning minified code."	
20	Public vulnerability search. See sections 4.2, Published Vulnerabilities, and 5.1, Public Vulnerability Search, for complete results.	The system is air-gapped—that is, not connected to the internet or connected to any other system that is connected to the internet. Air gap systems include • Ballot Marking Device Manager (BMG) • Ballot Marking Device (BMD) • VSAP Ballot Layout (VBL) • Tally The following security products are used to facilitate the air-gapped environment: • Carbon Black Protection: Provides application control to lock down critical systems in order to prevent unwanted software changes and malicious attacks. • CylancePROTECT: Threat prevention	Smartmatic staff has investigated this list of potential software security vulnerabilities. We find that most of these relate to Internet connected systems. Some could be exploited by trusted insiders, even without the system being inadvertently or maliciously attached to the Internet. We note that many are not easy to exploit or would not give an attacker meaningful access or capabilities that would allow undetectable manipulation or results or denial of service. A malicious trusted insider would likely attempt other avenues by which to subvert the voting system. We would like to point out that the entire certification candidate VSAP voting system remains under contracted Warranty for two years, and optional (Los Angeles County carries the option) Maintenance beyond that timeframe. These listed software vulnerabilities as well as others that might be found in the future by researchers would be dangerous if the product is off support, meaning that no one is available to assess the vulnerability and remediate it if deemed necessary. CVSS speaks to the possibility that new, unforeseen vulnerabilities in voting systems may emerge during the system lifecycle. In several places (9.6.d and 9.6.3.g as two examples) CVSS requires planning to respond to new threats. Los Angeles County has fulfilled the letter and spirit of these clauses by	Low

#	Description	Assessment	Developer Response	Severity
		solution (anti-virus) which utilizes machine-learning, allowing the software to function in isolation from the internet or cloud connection. • HP Aruba ClearPass: Tracks machine (MAC) addresses of all network cards on the network and can remove unauthorized addresses. • Net Fort LANGuardian: Tracks movement of all software, users, and actions on the network. • Snare System Information and Event Management (SIEM): Records all computer system and network activities, which are available for review in the event of an attack or issue. • Thycotic Secret Server: Manages all administrative privileged network accounts and limits users to standard access, limiting	ensuring that their System Integrator remains responsible for system maintenance. At this late time in the Certification campaign, we do not see the ability to remediate the listed software vulnerabilities assuming any could be exploited and would serve as a valuable target. Where deemed necessary by Los Angeles County, the system owner and operator, or the Secretary of State vulnerabilities will be remediated under the established system Warranty contract clauses.	

#	Description	Assessment	Developer Response	Severity
		opportunities for software changes. Note: Unused hardware ports (i.e. USB ports) are protected by port locks and/or tamper evident seals with signaling residue to reveal modification and/or removal. The serialized tamper evident seals are manually logged with an operator signature, seal number, location, date and time. This is to prevent removal of authorized connections when the port is in use and to prevent the insertion of unauthorized connections when the port is not in use. This prevents any infected USB flash drive from crossing any air gap.		
21	The CA certificate and key are stored in tmp and set to 777 file permissions. Programmatic copy of the CA cert and key to the cluster machines makes sense as its going to be necessary for later steps in the process, but in this case the file is set to 777 permissions, which means that all users have all permissions on these files. While it's possible that Kubernetes requires liberal file permissions for its CA cert and key, the go script does not delete the source files. Thus, the CA key could be stolen and used to	Programmatic setting of permissions to highly open configuration, and source files are not deleted after being copied to destinations on cluster machines. Leaving a copy of the CA key in the temp folder of a multi-user operating system is an incorrect configuration of a CA or	"In practice, this isn't a significant risk as, although the operating system is multi-user, the machine cluster is single tenant running only the Tally (or VBL) system and only administrators on the Tally system should be authorized on the environment. Mitigation ● The documentation will be updated to instruct the installer user to delete all data from temp once the install is finished. ● A procedure has been added to restrict file system permissions on these files	Low

#	Description	Assessment	Developer Response	Severity
	falsify certificates.	PKI infrastructure. Industry standard processes dictate that the root CA is created and stored on an air-gapped system, and intermediate CA's used to further certificate generation on destination machines. If this is the root CA in particular, then this is an inappropriate use case. If nothing else, the environment should be cleaned to prevent the CA from falling into the wrong hands.	post-install."	
22	Point of origin is not taken into consideration with authentication entries. Authentication with MySQL can also factor in point of origin which should be used to prevent unauthorized attempts to login. The SQL template allows authentication to the MySQL host from any other host for all users defined. The template file uses the standard syntax of '%' to signify the any host wild card for users being inserted into the database.	This configuration could allow someone to systematically try different authentication combinations until a valid one is found, leading to invalid voting data. Unless it's crucial that all users can login from all hosts, then the default template is too liberal in its use and definitions of who can login from where.	"The user must be able to log in from a docker container on one of several (currently about 9) kubernetes cluster machines. Moving forward, we can look at ways to limit this host list, but at present this would appear to require making some significant assumptions about the details of the production environment (such as IP addresses) that pose a challenge. Moving forward we will look for better options to lock this down. We may be able to implement a manual procedure for more specific grants if this is deemed a high priority issue."	Low
23	Programmatic modification of SELinux parameters on entire cluster decreases the overall security of the cluster. SELinux is a value-added feature of RedHat based systems that prevents a number of security holes and other vulnerabilites from	Programmatic downgrade of security on hosts potentially increases the possible attack vectors by a malicious user on the entire cluster.	"The Tally and VBL systems, as a part of the hardening procedure get Carbon Black loaded on in high enforcement mode. With Carbon Black in place, it was determined that SELinux was redundant and so it was removed."	Non (reduced from low due to response)

#	Description	Assessment	Developer Response	Severity
	being exploited by an attacker by nature of its kernel based implementation. func (n *Node) SetSELinuxToPermissive uses SSH to login to remote hosts, and configures the machine's SELinux implementation to permissive mode.	SELinux can get in the way of certain work or jobs, but the use of audit2allow prevents the need to programmatically turn off a security feature such as this in the cluster. While it can be troublesome to work with, its purpose is to prevent many different attack vectors that can not be factored into a standard system configuration process. Placing SELinux into permissive mode is not advised, and can be configured to work with docker and other applications via audit2allow.		
24	Python 2 reaches end of life at the end of this year and will not be supported after 2019-12-31. Any future security vulnerabilities found in Python 2 will not be fixed. The document VSAP-TDP-012_Approved_Parts_List.pdf indicates both Python 2 and Python 3 are used. If Python 2 is a dependency, the product uses a language that is no longer supported after January 1, 2020.	While this does not represent an actual vulnerability, it has the potential to cause one in the future. Python 2 will not be supported or updated starting January 1. If any security vulnerabilities are found after that date, not only could they put the voting system at risk, they would most likely not be fixed. Developers should already be in the process of migrating code	"We reviewed open CVEs for Python 2.7 (the version used in the BMD) and found none that are scored in the 8, 9, and 10 range. We also note that the VSAP BMD remains under contracted Warranty for two years, and optional Maintenance beyond that timeframe. Python 2 vulnerabilities that might be found by researchers in the future would be dangerous if the product is off support, meaning that no one is available to assess the vulnerability and remediate it if deemed necessary. CVSS speaks to the possibility that new, unforeseen vulnerabilities in COTS products may emerge during the system lifecycle. In several places (9.6.d and 9.6.3.g as two examples) CVSS requires planning to respond to new threats.	Low

#	Description	Assessment	Developer Response	Severity
		to Python 3. Please see https://www.python.org/doc/sunset-python-2/ .	At this late time in the Certification campaign, we do not see the ability to move to Python 3 in the BMD software; however, we plan to fulfill the letter and spirit of CVSS and will monitor for new vulnerabilities in Python 2 during the Warranty phase of VSAP lifecycle. Where deemed necessary by Los Angeles County, the system owner and operator, or the Secretary of State new Python 2 vulnerabilities will be remediated under the Warranty contract clauses."	
25	Calico container securityContext set to privileged = true. securityContext: true is set for the container Calico, which controls network functions.	The potential problem with this configuration is simply that the container is running effectively as root. An attacker could use this to reboot the system, delete files, modify passwords, etc. The developer of the voting systems is off the hook for this setting; There is a bug report filed at the following URL, which is attempting to deal with this issue related to Calico: https://github.com/projectcalico/calico/issues/2000 That said, it should be mentioned as a future improvement for the voting system, as this level of access to a machine via container is unnecessary and dangerous.	"We agree that this is not an emergent finding but a future system version could see this remediated."	Low

#	Description	Assessment	Developer Response	Severity
26	Backdoor check. In reviewing the VSAP-TDP-004-01_Interface_Description.pdf document the interface definitions were reviewed for potential exploitation. After reviewing the code use of the interfaces no exploitation was found. I search of keywords that could lead to backdoors or exploitation was conducted with the following words: ghost, host, exit, shutdown, execute, connect, request, command, and send.	There were no findings of these words that could be used as a backdoor or to exploit the system.	No response required.	Non

Table 8: Summary of Issues Discovered During the Static Code Analysis

Appendix A: Response to Finding 3, Hard Coded Passwords

Table 9: Response to Finding 3, Hard Coded Passwords, details the response to each instance of a hardcoded password.

File	Description	Proposed Resolution
TDA1/auth-service/docker- compose.yml	Docker compose files are developer configurations and not used in production.	N/A
TDA1/ballot-layout/docker- compose.yml	Docker compose files are developer configurations and not used in production.	N/A
TDA1/ballot-layout/db/101_ auth_create_schema.sql	This user is a holdover from development. It will be removed.	This user will be removed from the SQL file.
TDA1/vbl_deployment/srv/sql/ schema/101_auth_create_schema.sql	This file is the deployment package version of the previous file.	See above
TDA3/auth-service/docker-compose.yml	Docker compose files are developer configurations and not used in production.	N/A
TDA3/tally-core/ballotreview-dc.yml	Docker compose files are developer configurations and not used in production.	N/A
TDA3/tally-core/dc-inject-sbrs.yml	Load testing tool only used in development.	N/A
TDA3/tally-core/docker-compose.yml	Docker compose files are developer configurations and not used in production.	N/A
TDA3/tally-core/mysql-dc.yml	Docker compose files are developer configurations and not used in production.	N/A
TDA3/tally-core/deployments/ kubernetes/inbjectsbr.yaml	Load testing tool only used in development.	N/A
TDA3/tally-core/deployments/ kubernetes/ dist/ ballotreview/ ballotreview.yaml	The installer will regenerate the YAML files in "...tally-core/ deployment/kubernetes/dist/*" based on "...tally-core/ deployment/ kubernetes/ templates/prod/*" These passwords/files are not used in production.	N/A
TDA3/tallycore/ deployments/ kubernetes/ dist/ core/ tallymanager.yaml	The installer will regenerate the YAML files in "...tally-core/ deployment/kubernetes/dist/*" based on "...tally-core/ deployment/ kubernetes/	N/A

	templates/prod/*" These passwords/files are not used in production.	
TDA3/ tally-core/ deployments/ kubernetes/ dist/ shared/ auth.yaml	The installer will regenerate the YAML files in "...tally-core/ deployment/kubernetes/dist/*" based on "...tally-core/ deployment/ kubernetes/ templates/prod/*" These passwords/files are not used in production.	N/A
TDA3/ tallycore/ deployments/ kubernetes/ dist/ shared/ mysql.yaml	The installer will regenerate the YAML files in "...tally-core/ deployment/ kubernetes/dist/*" based on "...tally-core/ deployment/ kubernetes/ templates/prod/*" These passwords/files are not used in production.	N/A
TDA3/tally-core/ scripts/ production/ dbseeder-dc.yml	Docker compose files are developer configurations and not used in production.	This script should be removed to avoid confusion.
TDA3/tally-core/ scripts/ production/ providers-docker-compose.yml	Docker compose files are developer configurations and not used in production.	N/A
TDA3/tally-core/ scripts/ production/ services-docker-compose.yml	Docker compose files are developer configurations and not used in production.	N/A
TDA3/tally_deployment/ srv/tally_root/ db/ cql/ schema/ dropAddDevUser.cql	This file is no longer used in production, we will remove it.	This script should be removed to avoid confusion.

Table 9: Response to Finding 3, Hard Coded Passwords

Glossary

AES	Advanced Encryption Standard
API	Application Programming Interface
BEL	BMD Election Logs
BMD	Ballot Marking Device
BMG	BMD Manager
CAPI	Crypto API
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off-The-Shelf
CPE	Common Platform Enumeration
CRC	Cyclic Redundancy Check
CTR	Counter
CVE	Common Vulnerability and Exposures
CVR	Cast Vote Record
CWE	Common Weakness Enumeration
TDES	Triple-Data Encryption Standard
EC	Elliptic Curve
ECDSA	Elliptic Curve Digital Signature Algorithm
EMS	Election Management System
ESA	Enterprise Signing Authority
FIPS	Federal Information Processing Standard
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure

IP	Internet Protocol
ISB	Interactive Sample Ballot
IV	Initialization Vector
KDF	Key Derivation Function
LAN	Local Area Network
MAC	
OS	Operating System
PBKDF	Password-Based Key Derivation Function
PC	Personal Computer
PKI	Public Key Infrastructure
PRF	Pseudo-Random Function
PRNG	Pseudorandom Number Generator
RAVBM	Remote Accessible Vote by Mail
RCV	Ranked Choice Voting
RMS	Removable Media Service
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standards
SOS	Secretary of State
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TDP	Technical Data Package
TLS	Transport Layer Security
TRD	Technical Requirements Document

USB	Universal Serial Bus
UOCAVA	Uniformed Overseas Citizens Absentee Voting Act
VAT	Voter Assist Terminal
VBL	VSAP Ballot Layout
VBM	Vote by Mail
VSAP	Voting Systems for All People
XML	Extensible Markup Language

References

Documentation provided for the source code review included VSAP product documentation and other publicly available standards documents. The atsec source code review team also consulted other publicly available documents listed in the last group.

VSAP Documents

Technical Specifications

Configuration Management Plan, Version 1, Draft B (07/15/2019)

Configuration Management Plan Conformity Matrix TDP, Version B, Draft B (07/15/2019)

System Overview TDP, Version 1, Draft C 10/14/2019

System Overview Conformity Matrix TDP, Version 1, Draft B (07/15/2019)

System Functionality Description TDP, Version 1, Draft B (07/15/2019)

System Functionality Description Conformity Matrix TDP, Version 1, Draft B (07/15/2019)

System Hardware Specification TDP, Version 1, Draft E (09/12/2019)

System Hardware Specification Conformity Matrix TDP, Version 1, Draft B (07/15/2019)

Software Design and Specification TDP, Version 1, Draft C (10/14/2019)

Software Design and Specification – Interface Description TDP, Version 1, Draft C (09/25/2019)

Software Design and Specification Conformity TDP, Version 1, Draft B (07/15/2019)

System Security Specification TDP, Version 1, Draft C (09/25/2019)

System Security Specification Conformity Matrix TDP, Version 1, Draft C (09/25/2019)

System Test and Verification Specification TDP, Version 1, Draft C (10/14/2019)

System Operations Procedures TDP, Version 1, Draft B (07/15/2019)

System Operations Procedures Conformity Matrix TDP, Version, Draft B (07/15/2019)

System Maintenance TDP, Version 1, Draft B (07/15/2019)

System Maintenance Conformity Matrix TDP, Version 1, Draft B (07/15/2019)

System Maintenance TDP, Version 1, Draft B (07/15/2019)

Personnel Deployment and Training Requirements Conformity Matrix TDP, Version 1, Draft B (07/15/2019)

Personnel Deployment and Training Requirements TDP, Version 1, Draft B (07/15/2019)

Configuration Audits Conformity Matrix TDP, Version 1, Draft A (07/15/2019)

Configuration Audits TDP, Version 1, Draft A (07/15/2019)

Acronyms and Definitions TDP, Version 1, Draft B (07/15/2019)

Approved Parts List TDP, Version 1, Draft C (11/18/2019)

User Guides

Use Procedures, Version 4 (11/2/2019)

Ballot Marking Device (BMD) User Guide, Version 4

Ballot Marking Device Manager (BMG) Installation Guide, Version 2

BMD Manager User Guide, Version 4 (10/23/2019)

BMD Solution Applications Build Procedures, Version 0.2 (10/14/2019)

BMD Solution OS Build Procedures, Version 0.4 (12/10/2019)

Carbon Black Agent Deployment for Windows – BMG, Version 0.2 (11/1/2019)

Carbon Black Enabling Protection – BMG, Version 0.2 (11/1/2019)

Carbon Black Uninstall Guide, Version 0.1 (11/4/2019)

Deployment Laptop Build Procedures, Version 0.1 (10/14/2019)

Digital Signing Authority (DSA) Server Build/Installation, Version 2

Digital Signing Authority (DSA) User Guide, Version 2

FormatOS Deployment Guide, Version 0.4 (11/1/2019)

Interactive Sample Ballot Pre-Processor User Guide, Version 4

Interactive Sample Ballot User Guide, Version 4

ISB Installation Guide, Version 0.1 (09/05/2019)

Secure Boot Tools Build Procedures, Version 0.3 (12/10/2019)

BMG Deployment Guide, Version 0.1 (07/16/2019)

Snare Server Installation Guide – BMG and Tally, Version 0.2 (11/1/2019)

Tally Build / Installation User Guide, Version 2

Tally User Guide, Version 2

Ubuntu Server Installation Guide, Version 0.1 (10/14/2019)

Ballot Layout Build / Installation User Guide, Version 2

Ballot Layout User Guide, Version 2

Carbon Black Server Installation Guide - BMG, Version 2.0 (11/1/2019)

Public Documents

California Voting System Standards, Published October 2014

National Institute of Standards and Technology, Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, January 2016, http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf

National Institute of Standards and Technology, FIPS 140-2 Security Requirements for Cryptographic Modules, May 2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

National Institute of Standards and Technology, FIPS 140-2 Annex A: Approved Security Functions, December 2002, http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf

National Institute of Standards and Technology, FIPS 180-4 Secure Hash Standard (SHS), March 2012, http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

National Institute of Standards and Technology, FIPS 186-4 Digital Signature Standard (DSS), July 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

National Institute of Standards and Technology, FIPS 197 Advanced Encryption Standard, November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

National Institute of Standards and Technology, FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC), July 2008, http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

National Institute of Standards and Technology, NIST Special Publication 800-57, Recommendation for Key Management—Part 1: General (Revised), January 2016, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

National Institute of Standards and Technology, NIST Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June, 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

National Institute of Standards and Technology, NIST Special Publication 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, November, 2015, https://csrc.nist.gov/publications/detail/sp/800-131a/rev-1/final